Rich's lesson module checklist

- □ Slides and lab posted
- □ WB converted from PowerPoint
- □ Print out agenda slide and annotate page numbers

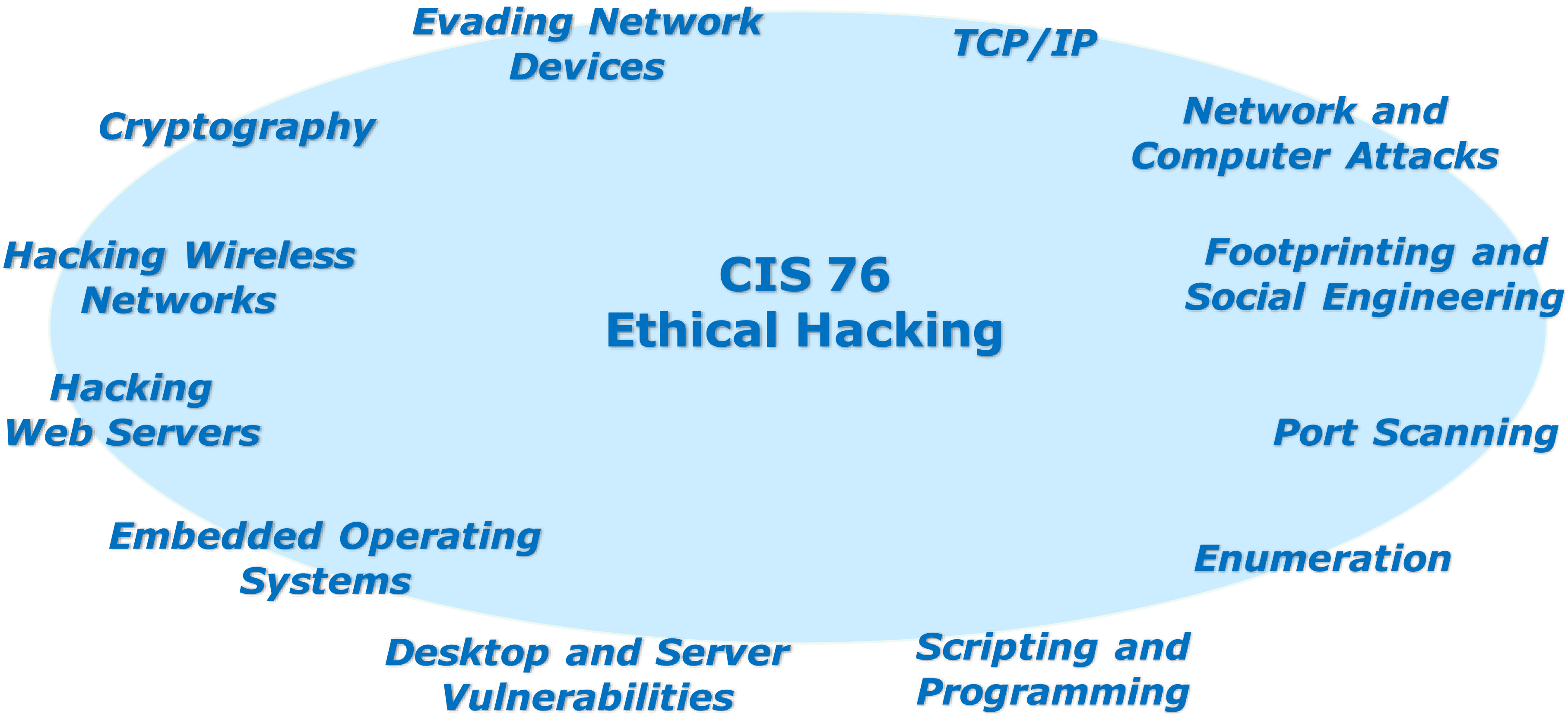
- □ Flash cards
- □ Properties
- □ Page numbers
- □ 1st minute quiz
- □ Web Calendar summary
- □ Web book pages
- □ Commands

- □ Project published

- □ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- □ Spare 9v battery for mic
- □ Key card for classroom door

- □ Update CCC Confer and 3C Media portals

Last updated 11/23/2016



Evading Network Devices

TCP/IP

Cryptography

Network and Computer Attacks

Hacking Wireless Networks

CIS 76
Ethical Hacking

Footprinting and Social Engineering

Hacking Web Servers

Port Scanning

Embedded Operating Systems

Enumeration

Desktop and Server Vulnerabilities

Scripting and Programming

Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

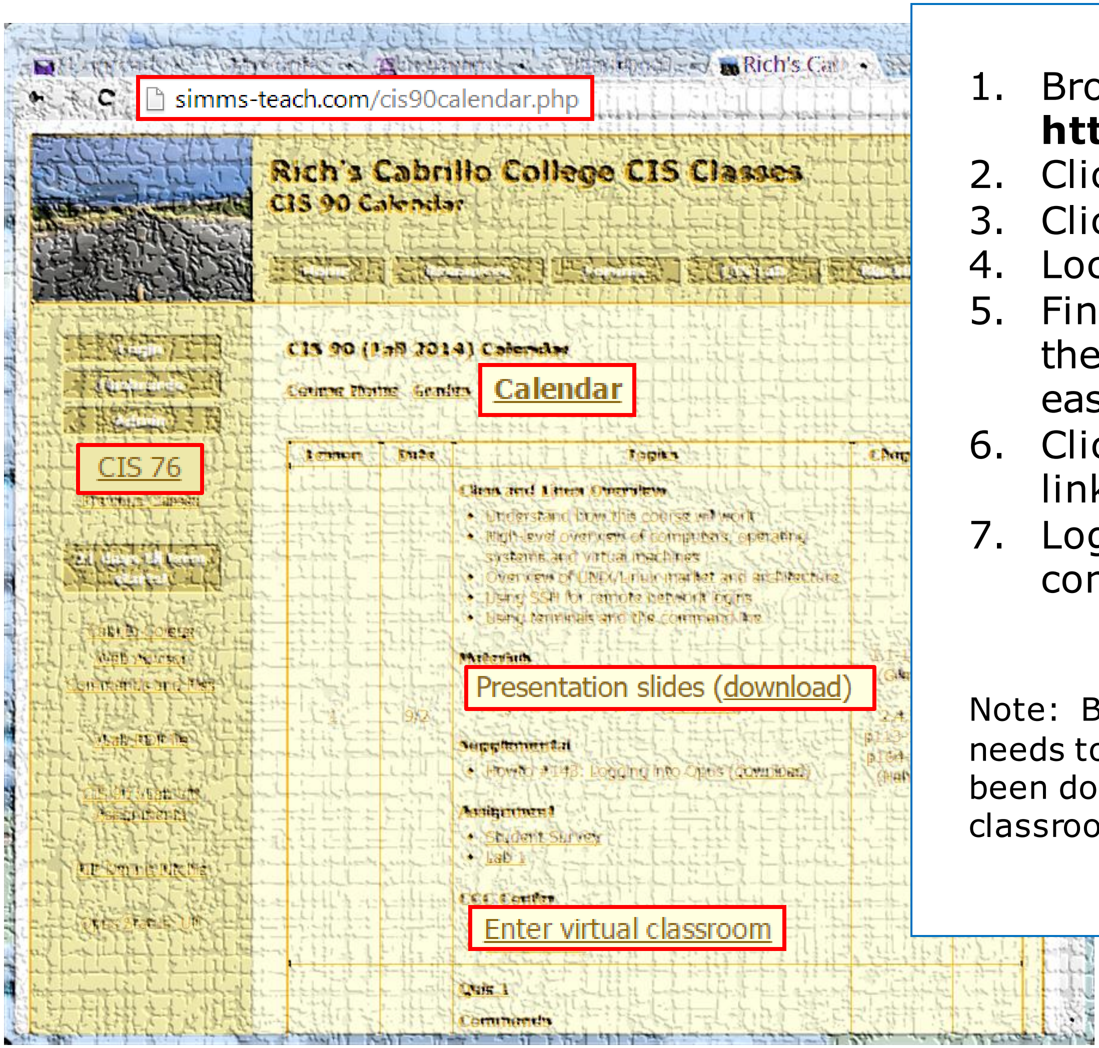
Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich’s site: http://simms-teach.com

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

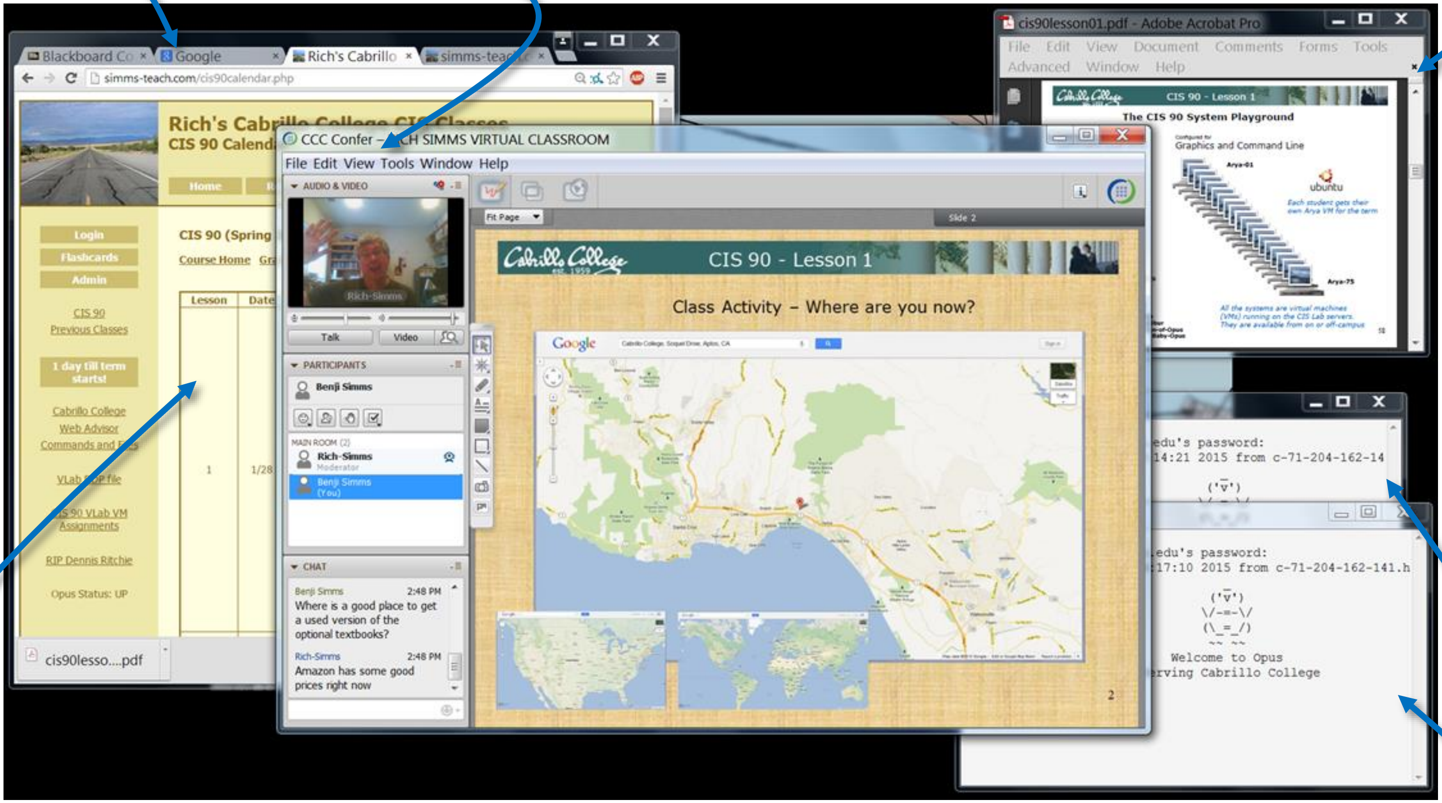

Rich's Cal
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

1. Browse to:
   http://simms-teach.com
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

- ❑ Google
- ❑ CCC Confer
- ❑ Downloaded PDF of Lesson Slides


Blackboard Co
Google
Rich's Cabrillo
simms-teach
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Home
Login
Flashcards
Admin
CIS 90
Previous Classes
1 day till term starts!
Cabrillo College
Web Advisor
Commands and Files
VLab RDP file
CIS 90 VLab VM Assignments
RIP Dennis Ritchie
Opus Status: UP
CIS 90 (Spring
Course Home
Lesson
Date
1
1/28
cis90lesso....pdf
CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Rich-Simms
Talk
Video
PARTICIPANTS
Benji Simms
MAIN ROOM (2)
Rich-Simms
Moderator
Benji Simms
(You)
CHAT
Fit Page
Slide 2
CIS 90 - Lesson 1
Class Activity – Where are you now?
Google
2
cis90lesson01.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
CIS 90 - Lesson 1
The CIS 90 System Playground
Graphics and Command Line
Arya-01
ubuntu
Each student gets their own Arya VM for the term
Arya-75
All the systems are virtual machines (VMs) running on the CIS Lab servers. They are available from on or off-campus
58

Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

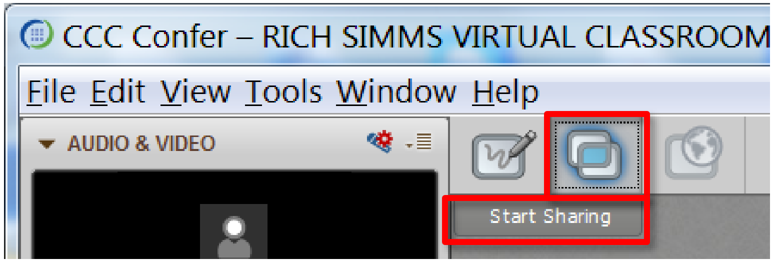
```
edu's password:
14:21 2015 from c-71-204-162-14
  ('v')
```

```
edu's password:
17:10 2015 from c-71-204-162-141.h
  ('v')
 \/-=-\/
  (\_=_/)
  ~~ ~~
  Welcome to Opus
erving Cabrillo College
```

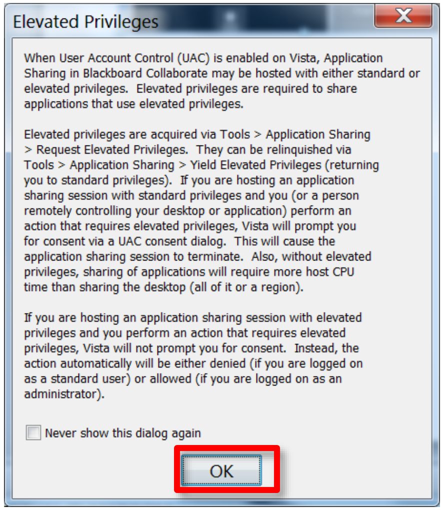
- ❑ CIS 76 website Calendar page
- ❑ One or more login sessions to Opus

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.


Elevated Privileges

When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

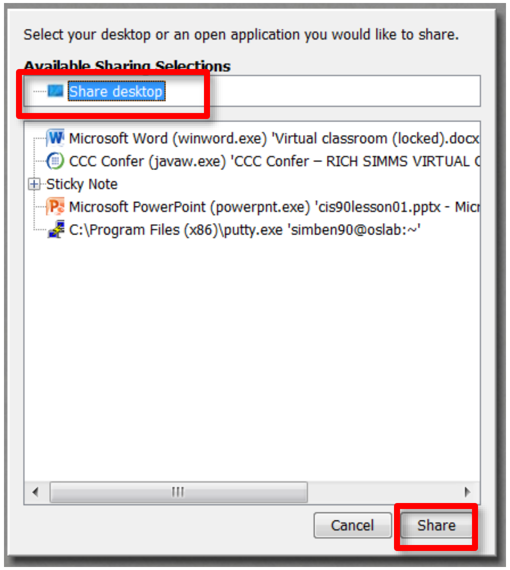
Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

☐ Never show this dialog again

OK

3) Click OK button.


Select your desktop or an open application you would like to share.

Available Sharing Selections

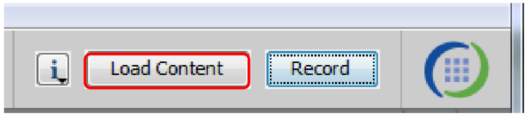
- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

Cancel Share

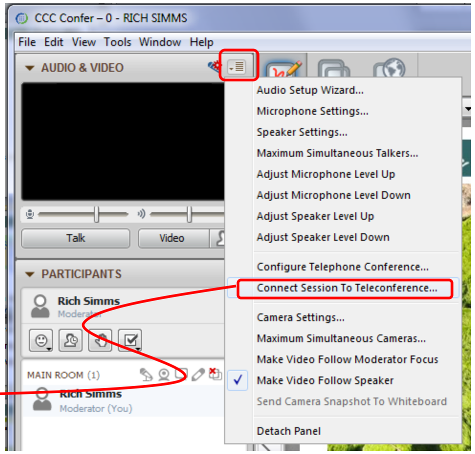
4) Select "Share desktop" and click Share button.

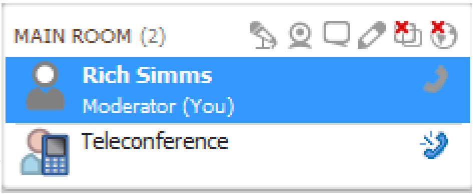
Rich's CCC Confer checklist - setup

[ ] Preload White Board



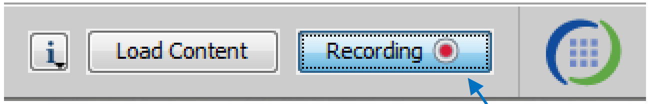
[ ] Connect session to Teleconference


CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)

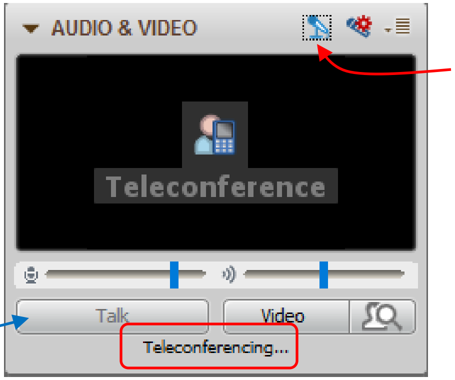


Session now connected to teleconference

[ ] Is recording on?



Red dot means recording

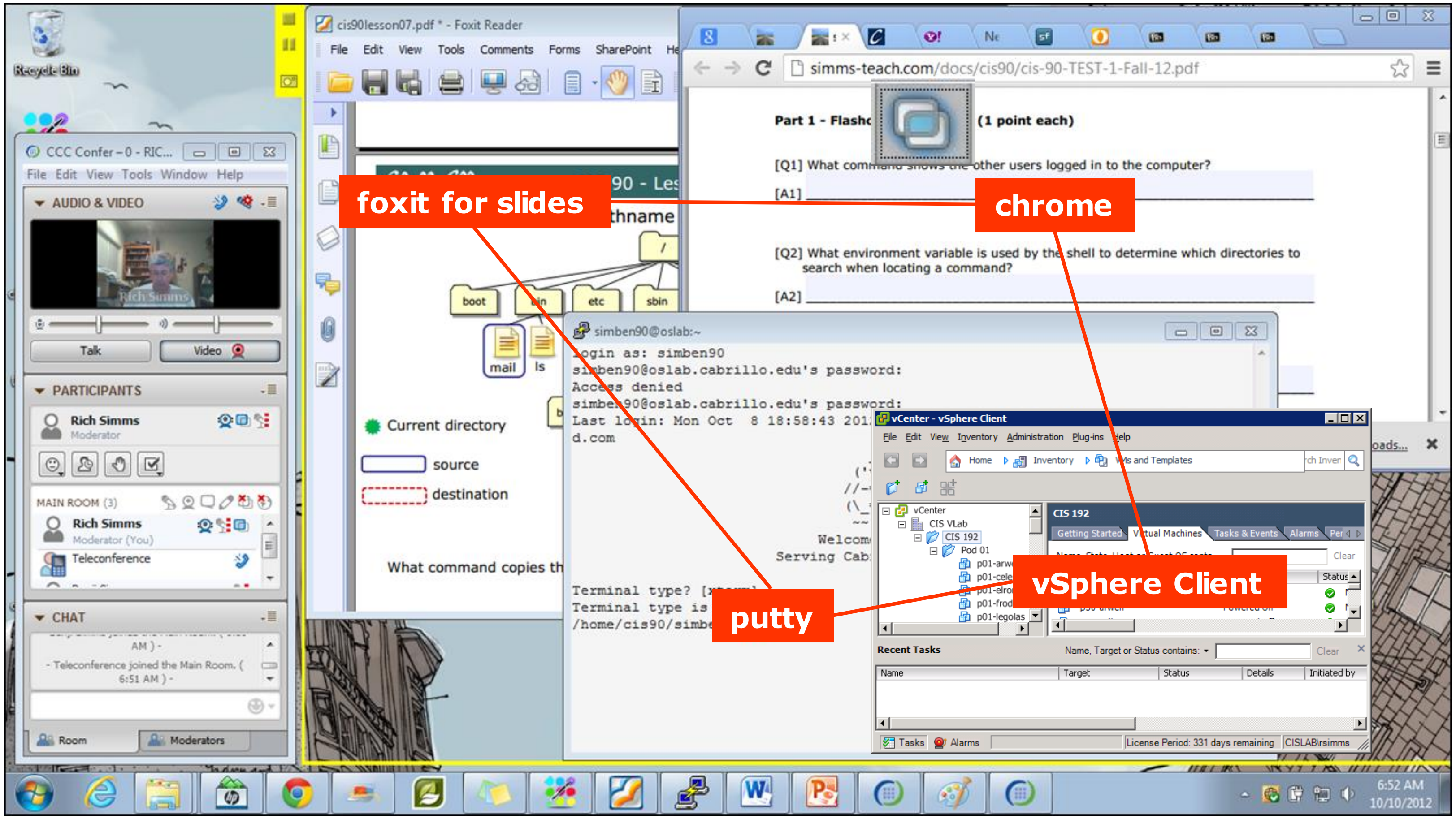


Should change from phone handset icon to little Microphone icon and the Teleconferencing ... message displayed

[ ] Use teleconferencing, not mic

Should be grayed out

Rich's CCC Confer checklist - screen layout



simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc (1 point each)

[Q1] What com other users logged in to the computer?

[A1] ______________________________

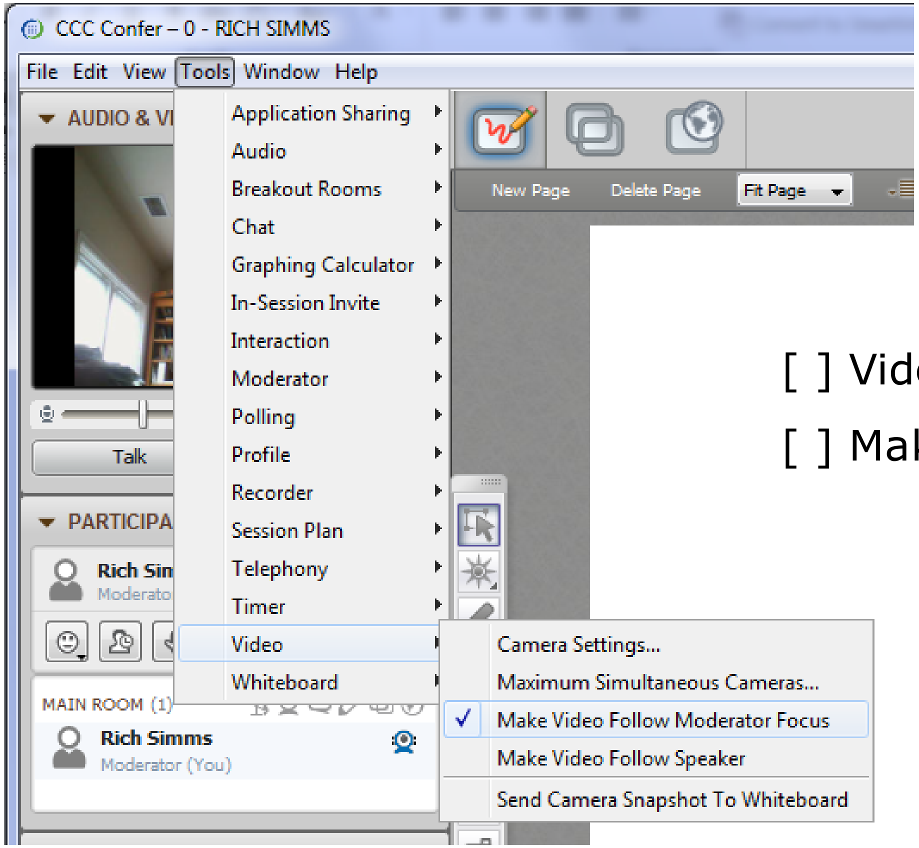
[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ______________________________

```
simben90@oslab:~
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

                                   Welcom
                                 Serving Cab

Terminal type? [x
Terminal type is
/home/cis90/simbe
```

[ ] layout and share apps

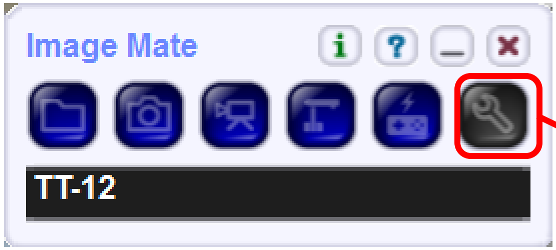
Rich's CCC Confer checklist - webcam setup

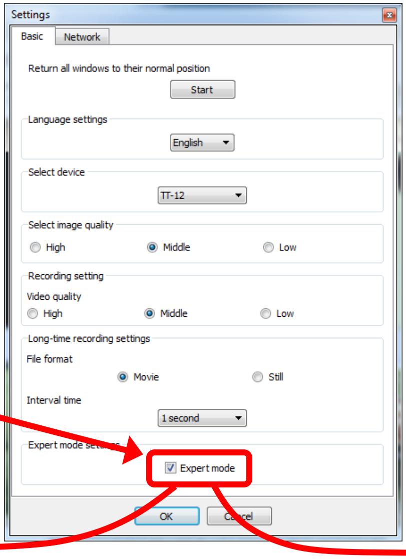


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode settings

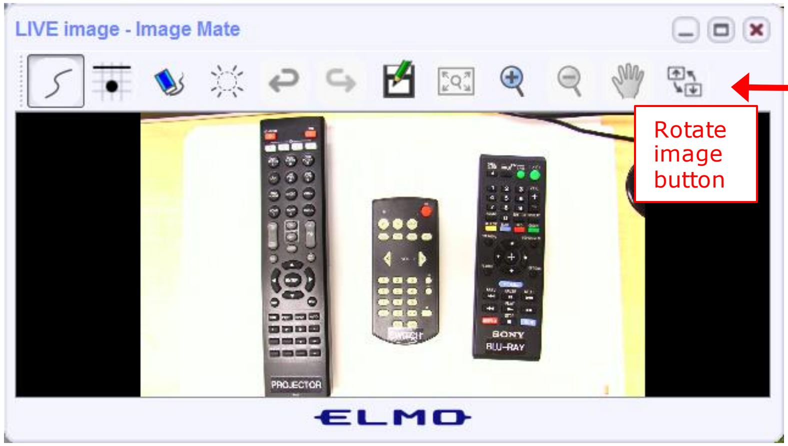
☑ Expert mode

OK | Cancel

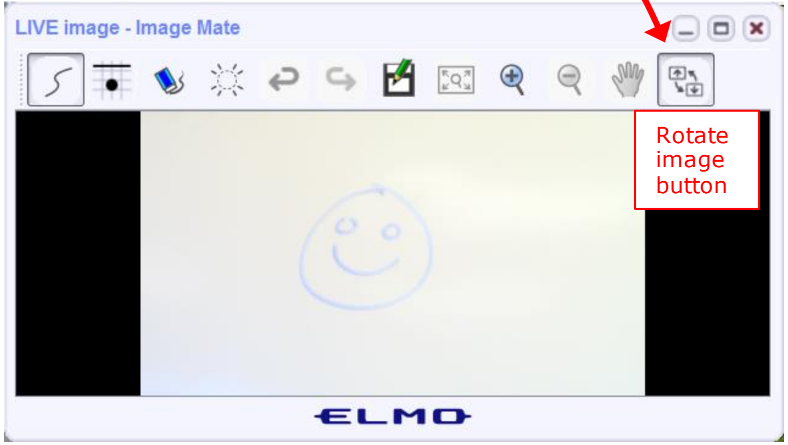
The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



Elmo rotated up to view white board



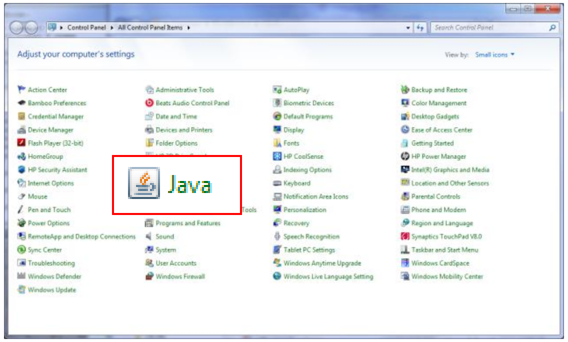
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

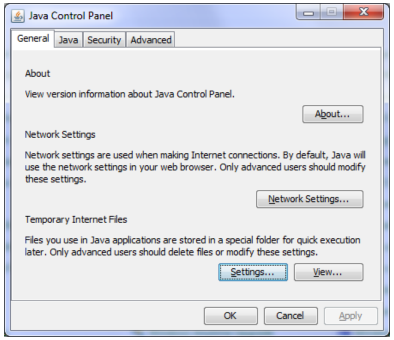
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

Control Panel (small icons)



General Tab > Settings...



About

View version information about Java Control Panel.

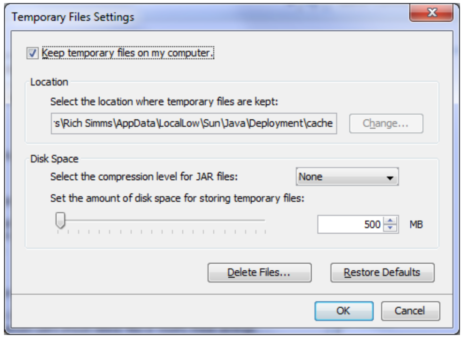
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size



☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

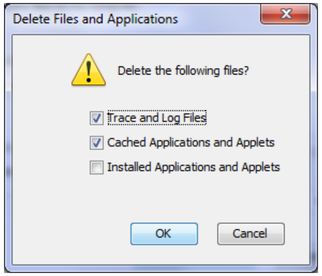
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

Delete these



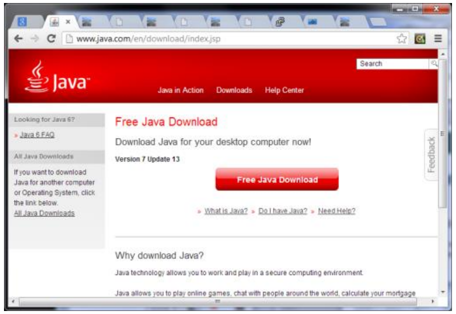
Delete the following files?

☑ Trace and Log Files

☑ Cached Applications and Applets

☐ Installed Applications and Applets

Google Java download



If you want to download Java for another computer or Operating System, click the link below.

All Java Downloads

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**

Ryan

Jordan

Takashi

Michael W.

Sean

Tim

Luis

Brian

Carter

Dave R.

David H.

Roberto

Nelli

Mike C.

Deryck

Alex

Thomas

Wes

Jennifer

Marcos

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

First Minute Quiz

Please answer these questions **in the order** shown:

Shown on CCC Confer

For credit email answers to:

`risimms@cabrillo.edu`

within the **first few minutes of the live class**

Hacking Wireless Networks

Objectives

- Explain wireless technology
- Describe wireless networking standards
- Describe wireless authentication
- Use some wireless hacking tools

Agenda

- Quiz #10
- Questions
- In the news
- Best practices
- Final project
- Housekeeping
- Wireless adapters and utilities
- Hacking WEP
- Hacking WPA/WPA2
- Assignment
- Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions

How this course works?

Past lesson material?

Previous labs?

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

Recent news

The value of anti-virus tools

http://www.theregister.co.uk/2016/11/17/google_hacker_pleads_try_whitelists_not_just_bunk_antivirus_ids/

- Google senior security engineer Daren Bilby.
- Responsible for researching advanced attacks.
- Advocates less effort on AV & IDS and more on whitelisting applications.
- "Antivirus does some useful things, but in reality it is more like a canary in the coal mine."
- Telling users not to click on phishing links shifts blame to them rather than the products that are not secure enough to be used online.
- He advocates focusing on whitelisting, hardware security keys and dynamic access rights.

Recent news

Qualcomm offering bug bounties up to $15,000

http://www.androidpolice.com/2016/11/17/qualcomm-offers-up-to-15000-in-bug-bounties-for-snapdragon-chipsets/

- Qualcomm makes wireless technology products including processors, chipsets, cellular modems, Bluetooth and WiFi.
- For disclosed vulnerabilities in Snapdragon chipsets, LTE modems and Android MSM Linux.
- Administered by cooperation with HackerOne.
- Must be new bugs and exclusively submitted.

Recent news

Inside job attacks 133,827 mobile accounts

http://www.theinquirer.net/inquirer/news/2477711/three-hack-six-million-customers-private-data-at-risk-after-inside-job-breach

- Three is a UK mobile operator.
- Hackers used an employee login to gain access.
- According to Three no payment information was accessed.
- They believe the objective was to fraudulently acquire new handsets not steal customer information.
- There have been eight fraudulent upgrades to new devices.
- The firm was fined 400,000 pounds last month by Britain's data protection regulator for security failings.
- Three suspects have been arrested.

Recent news

Hackers steal Mega.nz source code and admin logins

http://www.zdnet.com/article/hackers-say-they-took-mega-nz-admin-accounts-documents-source-code/

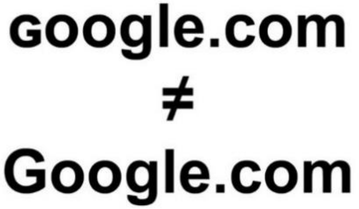
- Mega.nz is a file sharing site.
- The hacker group known as the Amn3s1a claimed responsibility.
- They first breached a developers system.
- Use privilege escalation and went on from there.
- The hacker group said: using a tool "that's not completely open source has big disadvantages".
- Mega.nz confirmed but downplayed the breach.

Recent news

Fake google.com domain

http://thenextweb.com/google/2016/11/21/google-isnt-google/

http://mashable.com/2016/11/21/fake-google-domain

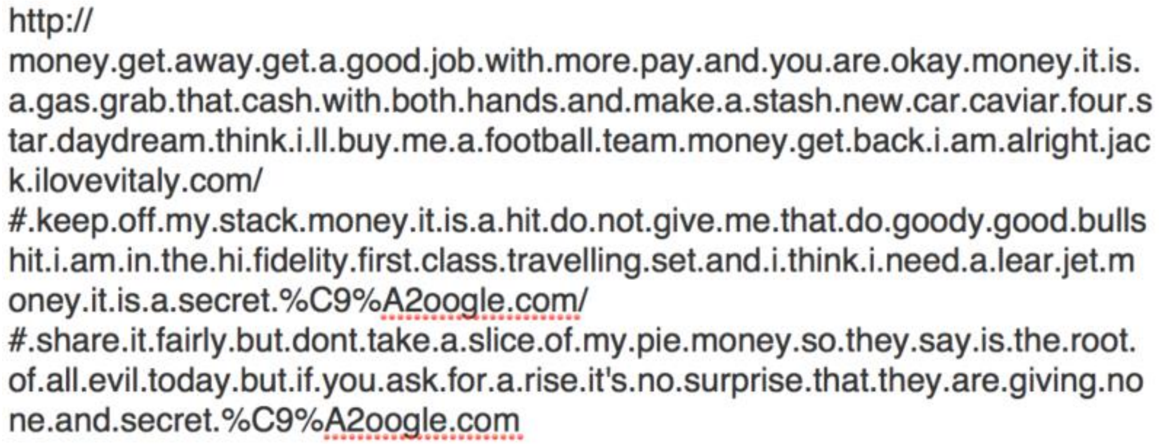


ɢoogle.com

≠

Google.com

- Unicode Character 'LATIN LETTER SMALL CAPITAL G' (U+0262)
- ɢoogle.com redirects to xn--oogle-wmc.com which redirects to:



http://
money.get.away.get.a.good.job.with.more.pay.and.you.are.okay.money.it.is.
a.gas.grab.that.cash.with.both.hands.and.make.a.stash.new.car.caviar.four.s
tar.daydream.think.i.ll.buy.me.a.football.team.money.get.back.i.am.alright.jac
k.ilovevitaly.com/
#.keep.off.my.stack.money.it.is.a.hit.do.not.give.me.that.do.goody.good.bulls
hit.i.am.in.the.hi.fidelity.first.class.travelling.set.and.i.think.i.need.a.lear.jet.m
oney.it.is.a.secret.%C9%A2oogle.com/
#.share.it.fairly.but.dont.take.a.slice.of.my.pie.money.so.they.say.is.the.root.
of.all.evil.today.but.if.you.ask.for.a.rise.it's.no.surprise.that.they.are.giving.no
ne.and.secret.%C9%A2oogle.com

Recent news

PoisonTap USB stick that installs backdoors on locked PCs and Macs

https://www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/?mbid=social_twitter

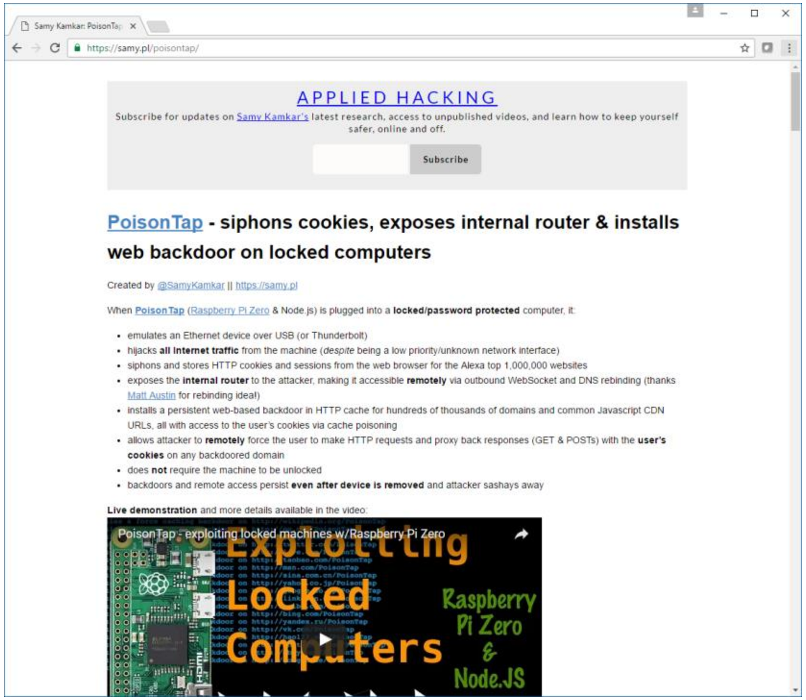
http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/

http://www.macrumors.com/2016/11/21/usb-device-hijacks-data-from-locked-macs/

- $5 Raspberry PI computer.
- Can be plugged into a locked or unlocked PC.
- Impersonates an Ethernet connection.
- Waits for a browser request then sends malicious code to the victim's browser cache.
- Created by Samy Kamkar who has released the schematics and code.

Recent news

https://samy.pl/poisontap/



APPLIED HACKING

Subscribe for updates on Samy Kamkar's latest research, access to unpublished videos, and learn how to keep yourself safer, online and off.

Subscribe

PoisonTap - siphons cookies, exposes internal router & installs web backdoor on locked computers

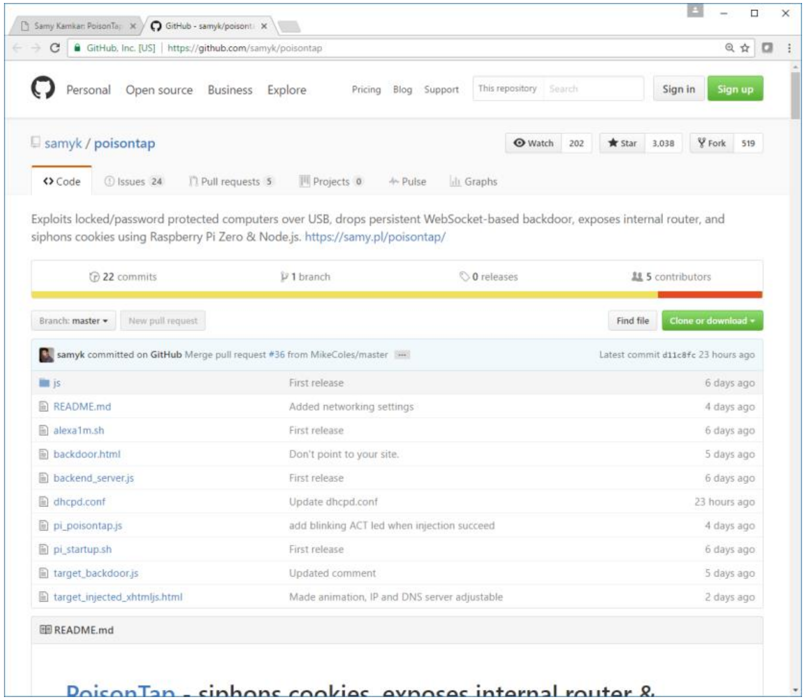
Created by @SamyKamkar || https://samy.pl

When **PoisonTap** (Raspberry Pi Zero & Node.js) is plugged into a **locked/password protected** computer, it:

- emulates an Ethernet device over USB (or Thunderbolt)
- hijacks **all Internet traffic** from the machine (*despite* being a low priority/unknown network interface)
- siphons and stores HTTP cookies and sessions from the web browser for the Alexa top 1,000,000 websites
- exposes the **internal router** to the attacker, making it accessible **remotely** via outbound WebSocket and DNS rebinding (thanks Matt Austin for rebinding idea!)
- installs a persistent web-based backdoor in HTTP cache for hundreds of thousands of domains and common Javascript CDN URLs, all with access to the user's cookies via cache poisoning
- allows attacker to **remotely** force the user to make HTTP requests and proxy back responses (GET & POSTs) with the **user's cookies** on any backdoored domain
- does **not** require the machine to be unlocked
- backdoors and remote access persist **even after device is removed** and attacker sashays away

Live demonstration and more details available in the video:

https://github.com/samyk/poisontap



samyk / poisontap

Exploits locked/password protected computers over USB, drops persistent WebSocket-based backdoor, exposes internal router, and siphons cookies using Raspberry Pi Zero & Node.js. https://samy.pl/poisontap/

22 commits | 1 branch | 0 releases | 5 contributors

samyk committed on GitHub Merge pull request #36 from MikeColes/master … Latest commit d11c8fc 23 hours ago

js	First release	6 days ago
README.md	Added networking settings	4 days ago
alexa1m.sh	First release	6 days ago
backdoor.html	Don't point to your site.	5 days ago
backend_server.js	First release	6 days ago
dhcpd.conf	Update dhcpd.conf	23 hours ago
pi_poisontap.js	add blinking ACT led when injection succeed	4 days ago
pi_startup.sh	First release	6 days ago
target_backdoor.js	Updated comment	5 days ago
target_injected_xhtmljs.html	Made animation, IP and DNS server adjustable	2 days ago

README.md

PoisonTap - siphons cookies, exposes internal router &

PoisonTap documentation and code

Best Practices

Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response

Software Engineering Institute
Carnegie Mellon University

SEI Blog

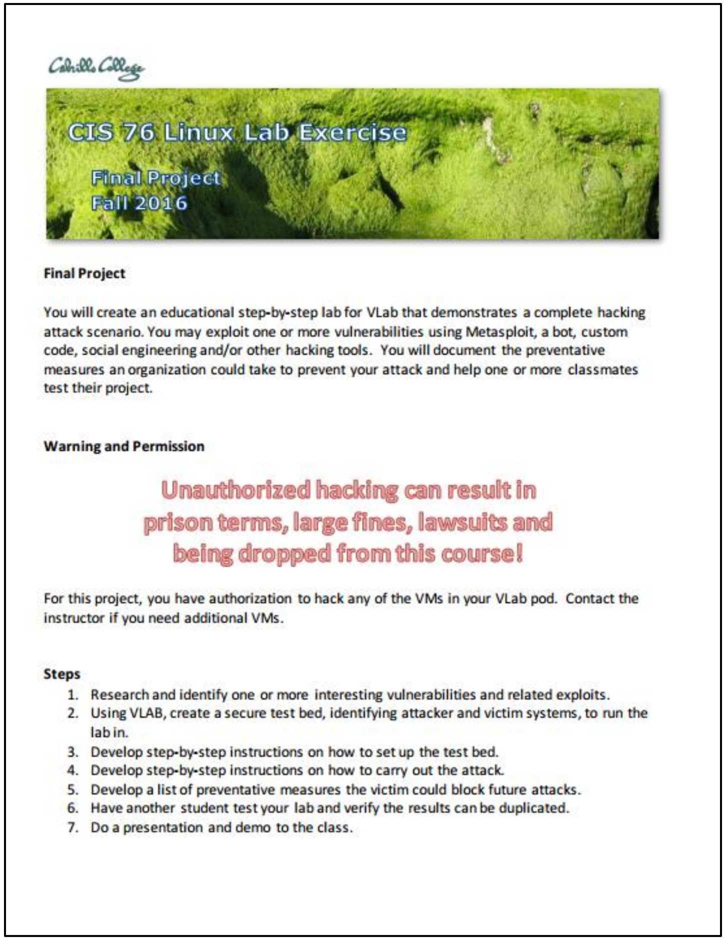
The Latest Research in Software Engineering and Cybersecurity

- Locate servers in different data centers.
- Ensure that data centers are located on different networks.
- Ensure that data centers have diverse paths.
- Ensure that the data centers, or the networks that the data centers are connected to, have no notable bottlenecks or single points of failure.

https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html

Final Project

CIS 76 Project



Cabrillo College

CIS 76 Linux Lab Exercise

Final Project
Fall 2016

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

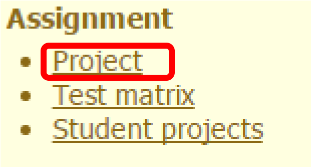
1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

The final project is available.

Due in two weeks.

Calendar Page

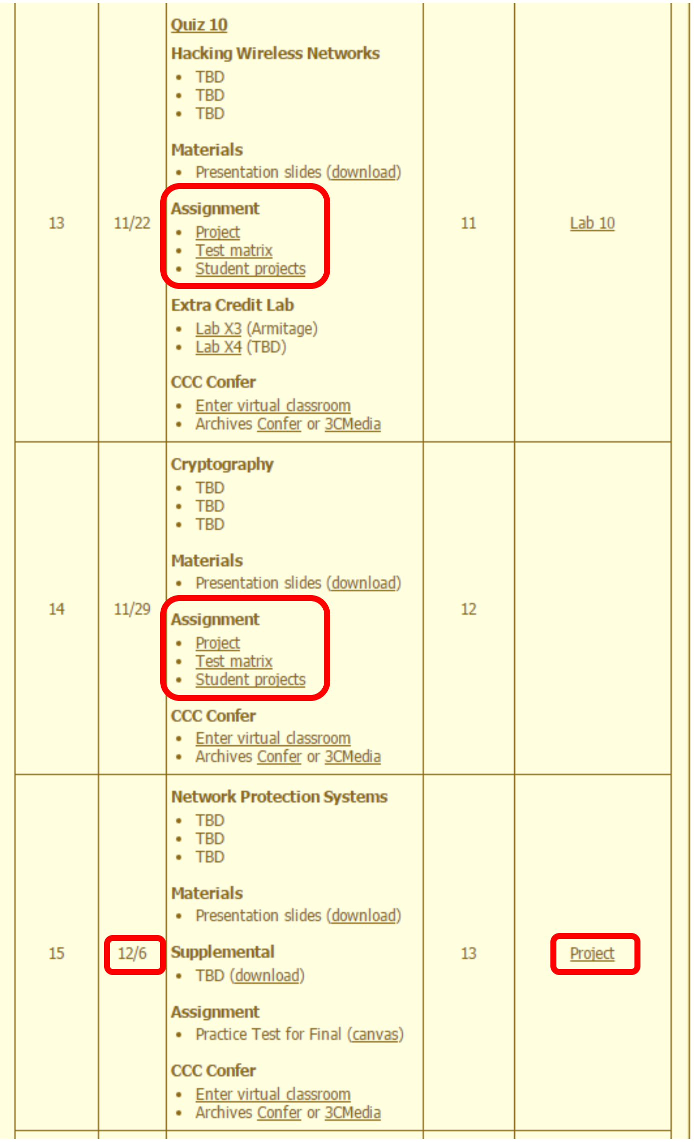


Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php

CIS 76 Project



13	11/22	Quiz 10 **Hacking Wireless Networks** - TBD - TBD - TBD **Materials** - Presentation slides (download) **Assignment** - Project - Test matrix - Student projects **Extra Credit Lab** - Lab X3 (Armitage) - Lab X4 (TBD) **CCC Confer** - Enter virtual classroom - Archives Confer or 3CMedia	11	Lab 10
14	11/29	**Cryptography** - TBD - TBD - TBD **Materials** - Presentation slides (download) **Assignment** - Project - Test matrix - Student projects **CCC Confer** - Enter virtual classroom - Archives Confer or 3CMedia	12	
15	12/6	**Network Protection Systems** - TBD - TBD - TBD **Materials** - Presentation slides (download) **Supplemental** - TBD (download) **Assignment** - Practice Test for Final (canvas) **CCC Confer** - Enter virtual classroom - Archives Confer or 3CMedia	13	Project

https://simms-teach.com/cis76calendar.php

Links to Project document, Test matrix, and online directory for students to share their projects from.

And again ...

Due 12/6

CIS 76 Project

Grading Rubric (60 points + 30 points extra credit)

Up to 5 points - Professional quality document containing all sections mentioned above.
Up to 3 points - Description and history of vulnerability.
Up to 3 points - Description of exploit and how it works.
Up to 3 points - Document all equipment, software and materials required.
Up to 10 points - Document step-by-step instructions to set up the test bed.
Up to 15 points - Document step-by-step instructions to carry out the attack.
Up to 3 points - List of best practices to prevent future attacks.
Up to 15 points - Testing another student's lab (see below).
Up to 3 points - Presentation and demo to class (10 minutes max).

Extra credit (up 30 points) 15 points each for testing additional student labs. You must use the testing spreadsheet above so that all projects get tested equally.

Remember late work is not accepted. If you run out of time submit what you have completed for partial credit.

Excerpt from the Project document

CIS 76 Project

Testing another classmate’s lab

1. Find a lab that hasn’t been tested yet and sign up on the testing spreadsheet.

2. Run through their entire lab and verify that it works properly.

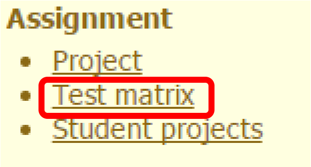
3. Provide the lab developer with a written test report on:

- □ Your name and the date & time testing was done.
- □ Validation that the lab worked or not.
- □ Any typos.
- □ Any portions of the lab that need clarification.
- □ Any portions of the lab that need to be fixed.
- □ Any other feedback on ways to improve the lab.

Excerpt from the Project document

CIS 76 Project

Calendar Page

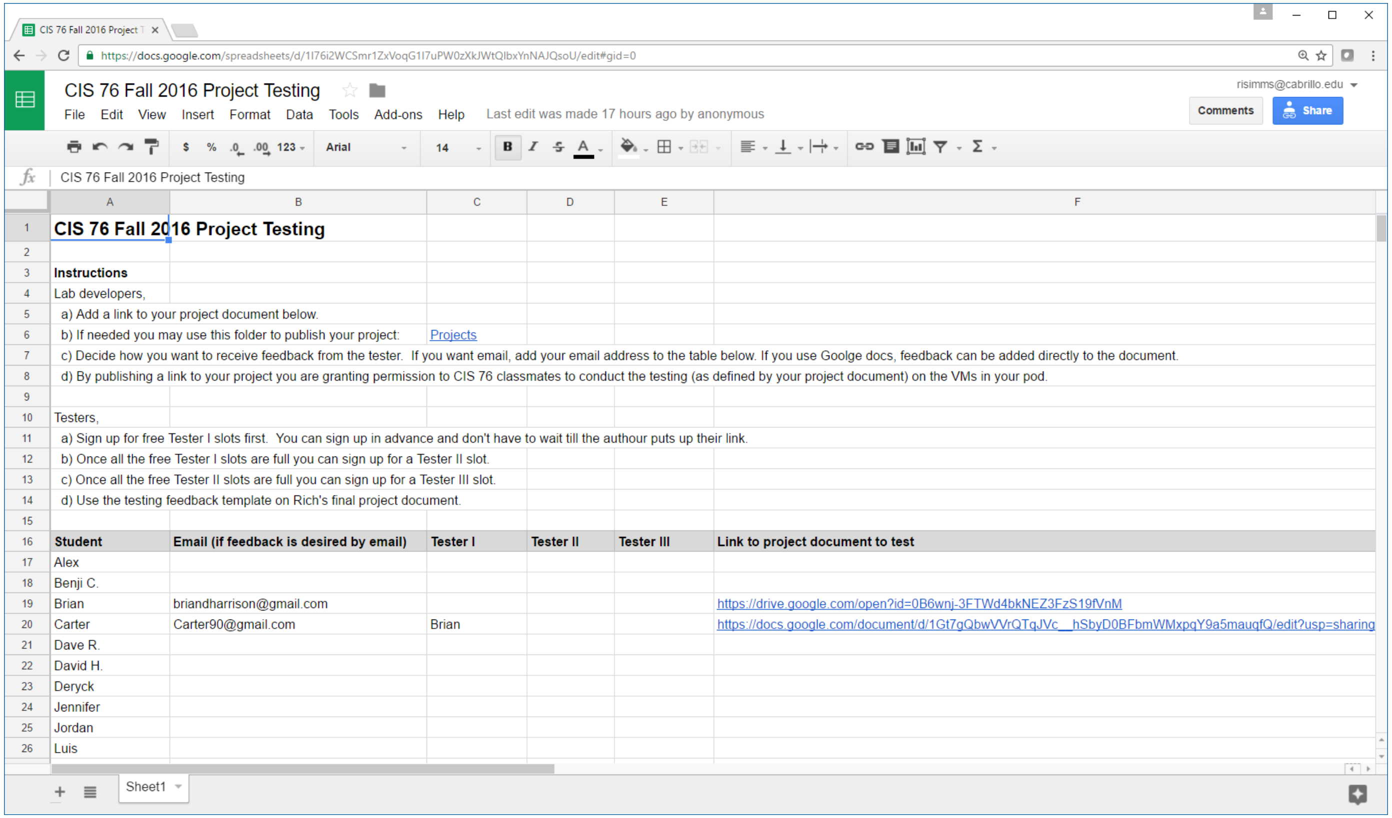


Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php

Use this Test matrix to sign up to test a classmate's project



CIS 76 Fall 2016 Project T ×
https://docs.google.com/spreadsheets/d/1I76i2WCSmr1ZxVoqG1I7uPW0zXkJWtQlbxYnNAJQsoU/edit#gid=0
risimms@cabrillo.edu
File Edit View Insert Format Data Tools Add-ons Help
Last edit was made 17 hours ago by anonymous
Comments
Share
$ % .0 .00 123
Arial
14
B I S A
fx CIS 76 Fall 2016 Project Testing
Sheet1

CIS 76 Fall 2016 Project Testing

Instructions

Lab developers,

a) Add a link to your project document below.

b) If needed you may use this folder to publish your project: Projects

c) Decide how you want to receive feedback from the tester. If you want email, add your email address to the table below. If you use Goolge docs, feedback can be added directly to the document.

d) By publishing a link to your project you are granting permission to CIS 76 classmates to conduct the testing (as defined by your project document) on the VMs in your pod.

Testers,

a) Sign up for free Tester I slots first. You can sign up in advance and don't have to wait till the authour puts up their link.

b) Once all the free Tester I slots are full you can sign up for a Tester II slot.

c) Once all the free Tester II slots are full you can sign up for a Tester III slot.

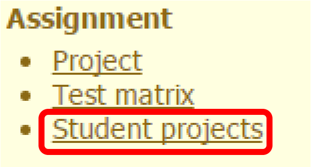
d) Use the testing feedback template on Rich's final project document.

Student	Email (if feedback is desired by email)	Tester I	Tester II	Tester III	Link to project document to test
Alex					
Benji C.					
Brian	briandharrison@gmail.com				https://drive.google.com/open?id=0B6wnj-3FTWd4bkNEZ3FzS19fVnM
Carter	Carter90@gmail.com	Brian			https://docs.google.com/document/d/1Gt7gQbwVVrQTqJVc__hSbyD0BFbmWMxpqY9a5mauqfQ/edit?usp=sharing
Dave R.					
David H.					
Deryck					
Jennifer					
Jordan					
Luis					

https://cabrillo.instructure.com/courses/4167/pages/cis-76-project-testing-signup-sheet

CIS 76 Project

Calendar Page

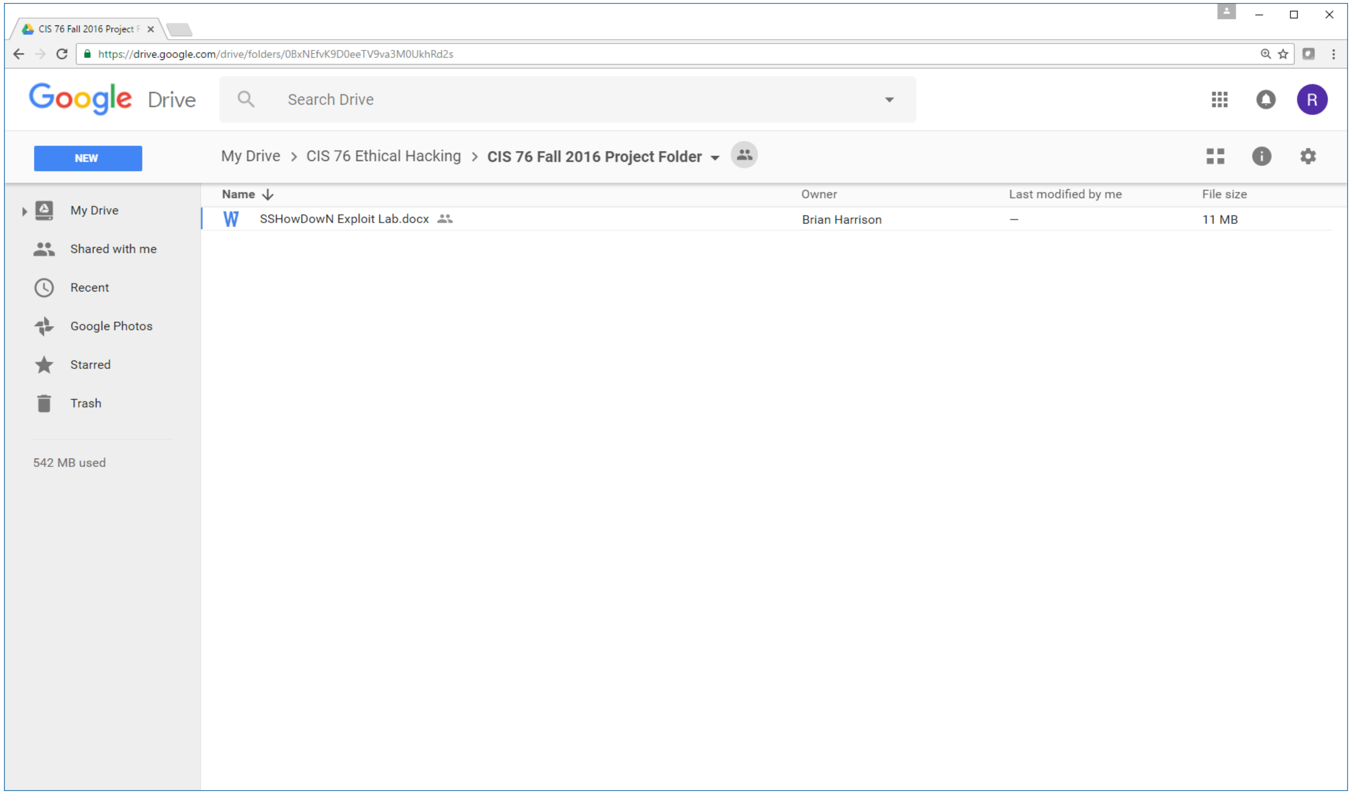


Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php

Use this directory to share your project with other classmates for testing



https://drive.google.com/drive/folders/0BxNEfvK9D0eeTV9va3M0UkhRd2s

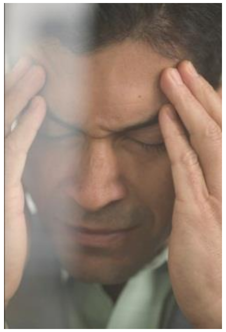
My Drive > CIS 76 Ethical Hacking > CIS 76 Fall 2016 Project Folder

Name	Owner	Last modified by me	File size
SSHowDowN Exploit Lab.docx	Brian Harrison	–	11 MB

https://cabrillo.instructure.com/courses/4167/pages/cis-76-project-folder

CIS 76 Project

What takes longer?



Creating the hacking project lab?

Or deciding what to project to do?

CIS 76 Project

Some Hacking Project Ideas

github projects

https://github.com/Hack-with-Github/Awesome-Hacking

EH-OWASP-XX VM

Chuck full of project ideas

Google searches

hacking tutorials

hacking projects

metasploit tutorials

kali hacking tutorials

ethical hacking tips

...

CVE Details

Find vulnerabilities with Metasploit modules

https://www.cvedetails.com/

Pick a project you can build in your CIS 76 EH pod

CIS 76 Project

And don't forget:

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

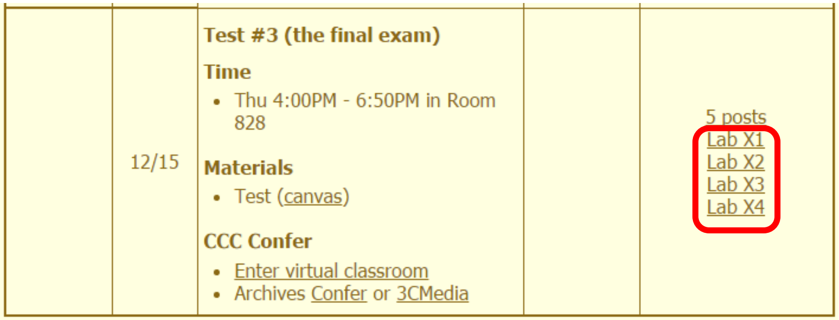
Housekeeping

war is not healthy for children and other living things
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
We're Proud To Serve

Housekeeping

1. Lab 10 due 11:59PM tonight.

2. All four extra credit labs are now available (15 points each) and due the day of the final exam.

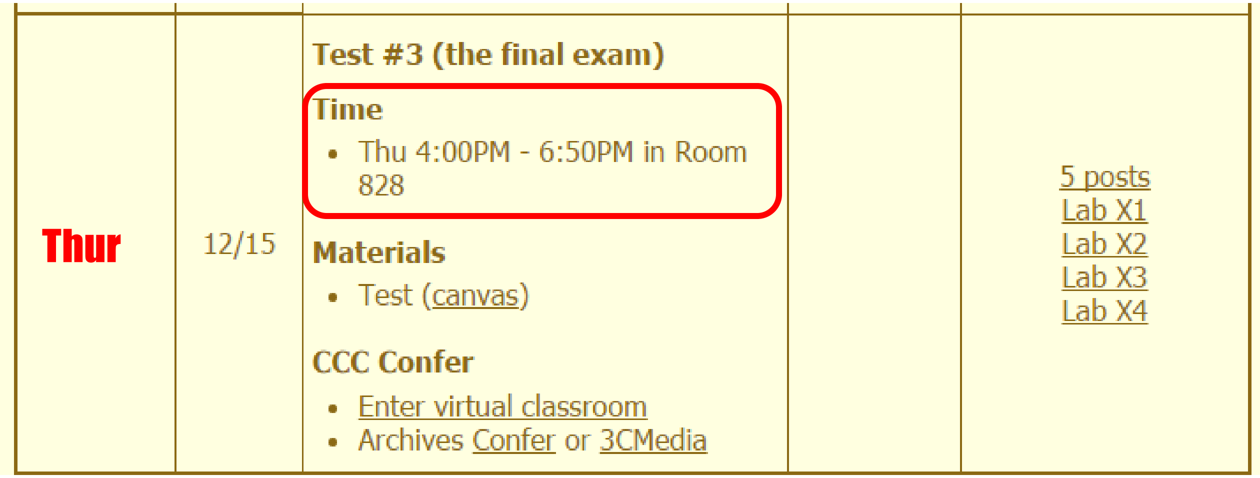


	12/15	**Test #3 (the final exam)** **Time** • Thu 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4

3. The final project is available now and due in two weeks.

Heads up on Final Exam

Test #3 (final exam) is THURSDAY Dec 15 4-6:50PM

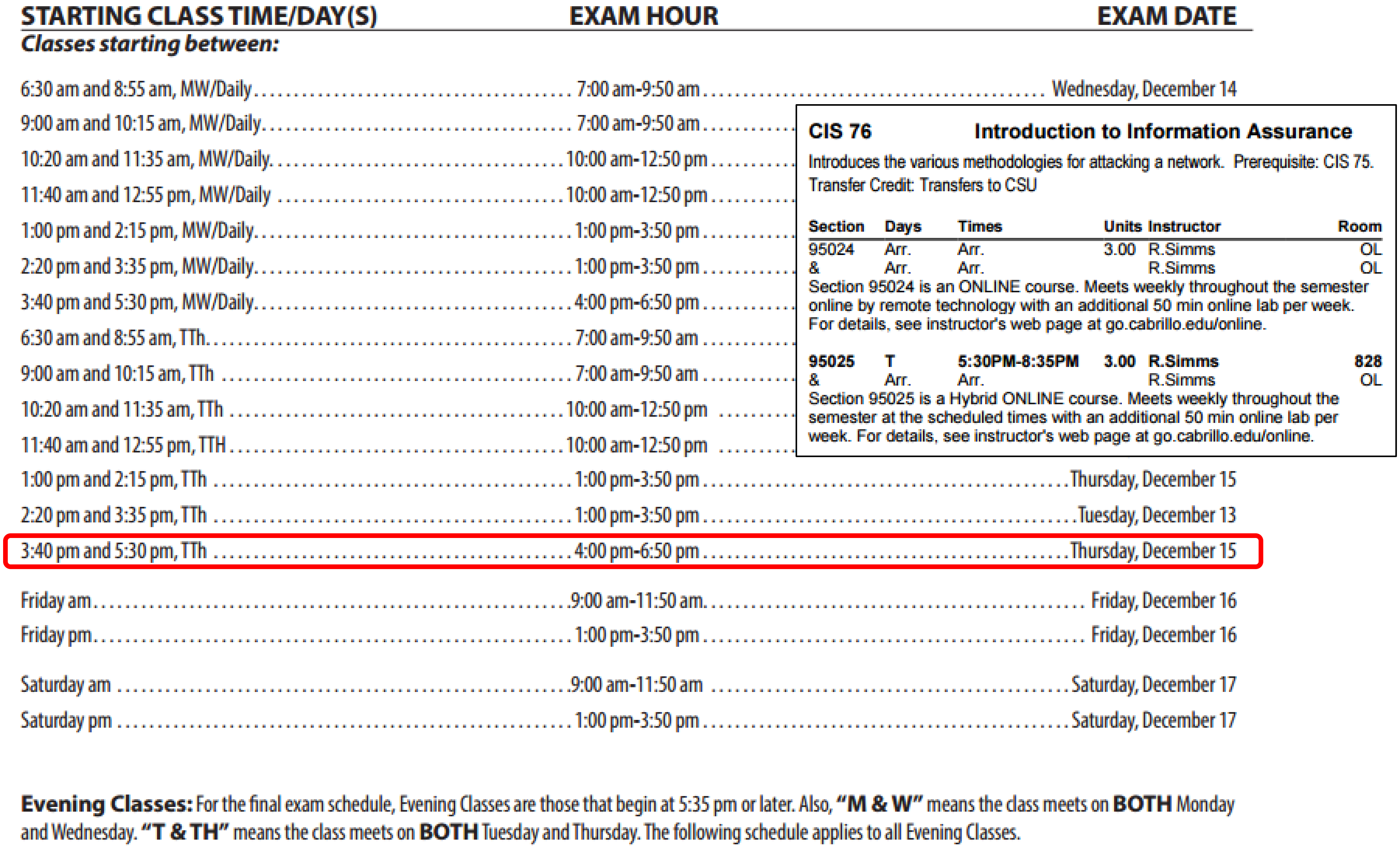


Thur	12/15	**Test #3 (the final exam)** **Time** • Thu 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4

Extra credit labs and final posts due by 11:59PM

- All students will take the test at the same time. The test must be completed by 6:50PM.
- Working and long distance students can take the test online via CCC Confer and Canvas.
- Working students will need to plan ahead to arrange time off from work for the test.
- Test #3 is mandatory (even if you have all the points you want)

CIS 76 - Lesson 13



STARTING CLASS TIME/DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 14
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Thursday, December 15
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 13
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Thursday, December 15
Friday am	9:00 am-11:50 am.	Friday, December 16
Friday pm	1:00 pm-3:50 pm	Friday, December 16
Saturday am	9:00 am-11:50 am	Saturday, December 17
Saturday pm	1:00 pm-3:50 pm	Saturday, December 17

Evening Classes: For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.

CIS 76 Introduction to Information Assurance

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75. Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL

Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Section	Days	Times	Units	Instructor	Room
95025	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

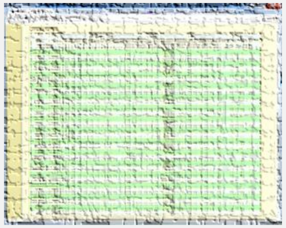
Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

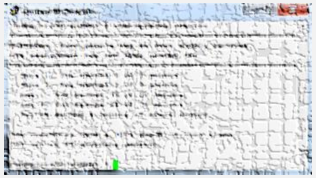
http://simms-teach.com/cis76grades.php



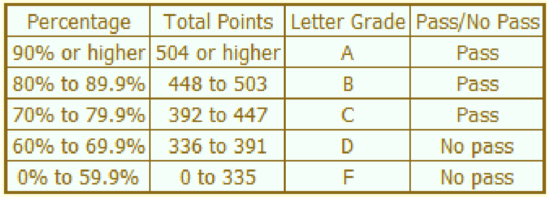
Or check on Opus

checkgrades *codename*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus



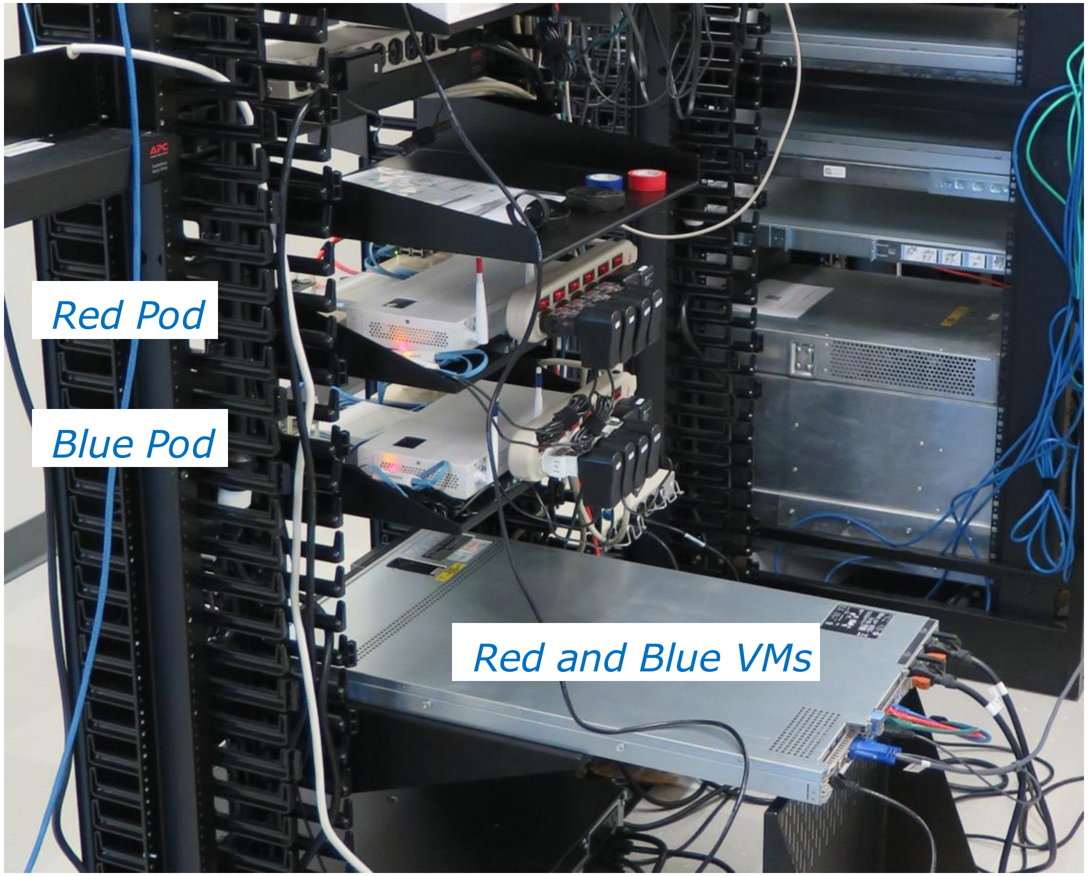
Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

At the end of the term I'll add up all your points and assign you a grade using this table

Points that could have been earned:	
9 quizzes:	27 points
9 labs:	270 points
2 tests:	60 points
3 forum quarters:	60 points
Total:	**417 points**

Red and Blue Teams

Red and Blue Pods in Microlab Lab Rack



Send me an email if you would like to join a team

Wireless

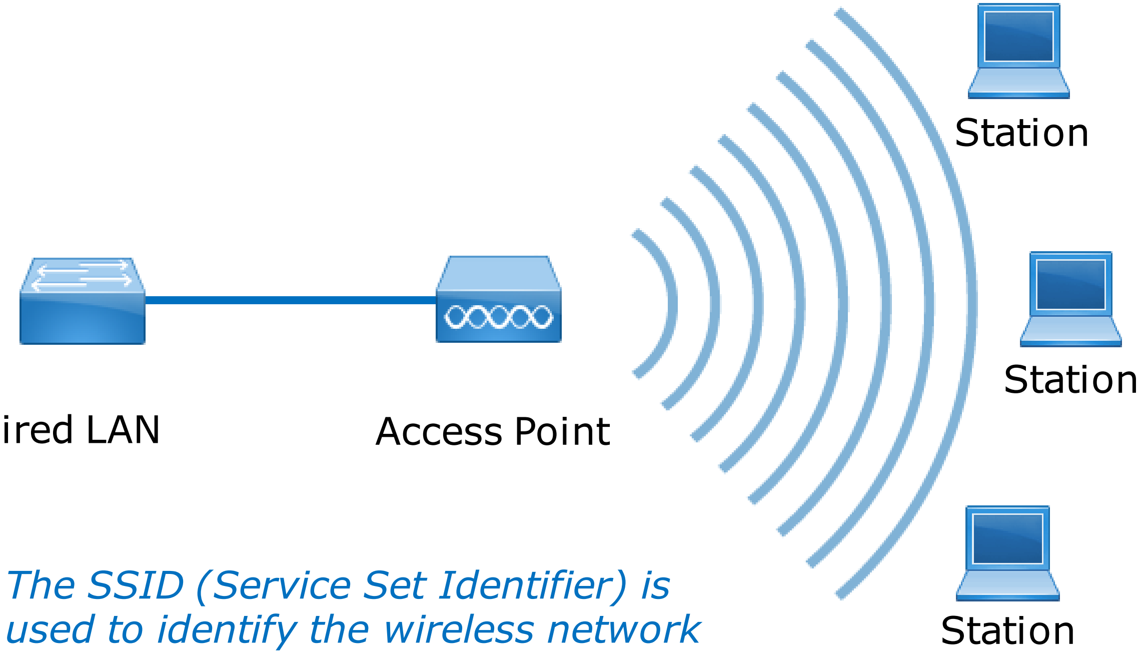
The World of Wireless Technology

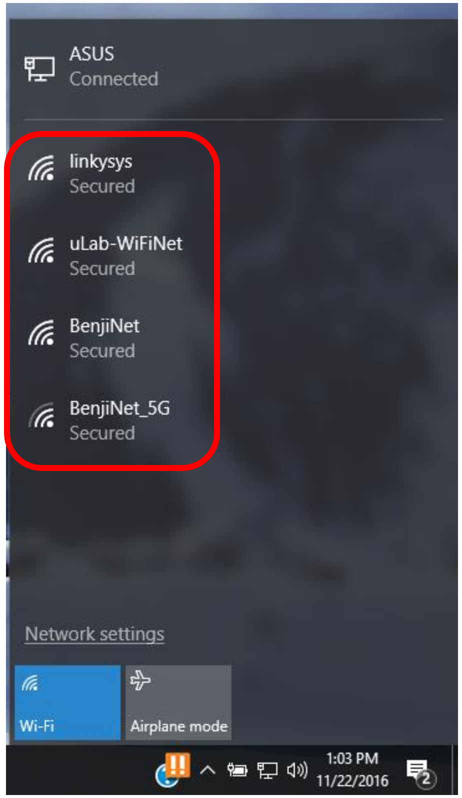
- Cell phones
- Cordless phones
- Smart phones
- Pagers
- Smart watches
- GPS
- Remote controls
- Garage door openers
- Car door openers
- Two-way radios
- Wireless laptops
- Tablets
- WiFi cams
- Fitbits
- And many more ...

Access Points

- Usually connected to a wired network

Devices with wireless network adapters configured to the SSID of the access point.




ASUS
Connected

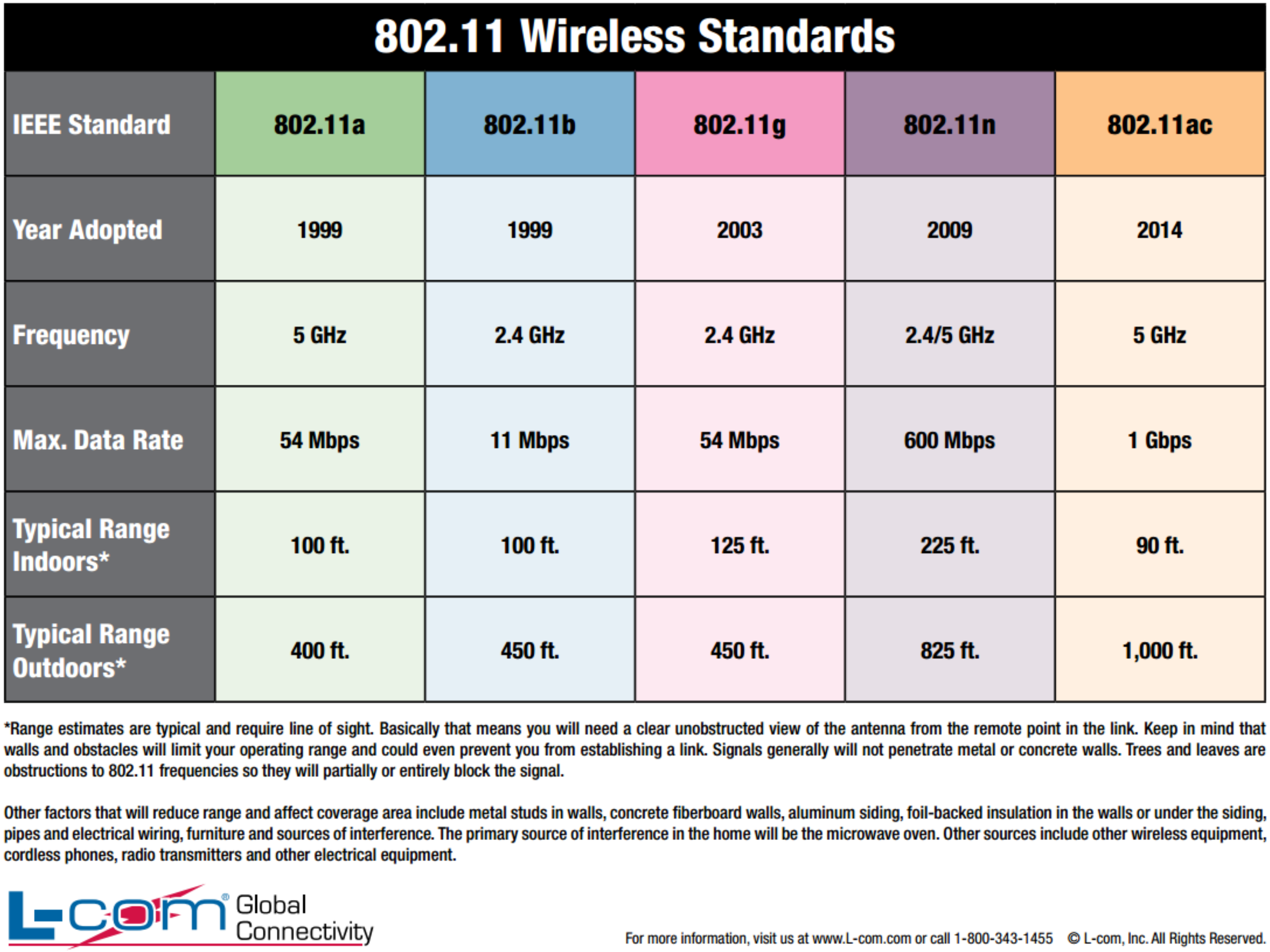
linkysys
Secured

uLab-WiFiNet
Secured

BenjiNet
Secured

BenjiNet_5G
Secured

The SSID (Service Set Identifier) is used to identify the wireless network and configured on the access point.



802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

*Range estimates are typical and require line of sight. Basically that means you will need a clear unobstructed view of the antenna from the remote point in the link. Keep in mind that walls and obstacles will limit your operating range and could even prevent you from establishing a link. Signals generally will not penetrate metal or concrete walls. Trees and leaves are obstructions to 802.11 frequencies so they will partially or entirely block the signal.

Other factors that will reduce range and affect coverage area include metal studs in walls, concrete fiberboard walls, aluminum siding, foil-backed insulation in the walls or under the siding, pipes and electrical wiring, furniture and sources of interference. The primary source of interference in the home will be the microwave oven. Other sources include other wireless equipment, cordless phones, radio transmitters and other electrical equipment.

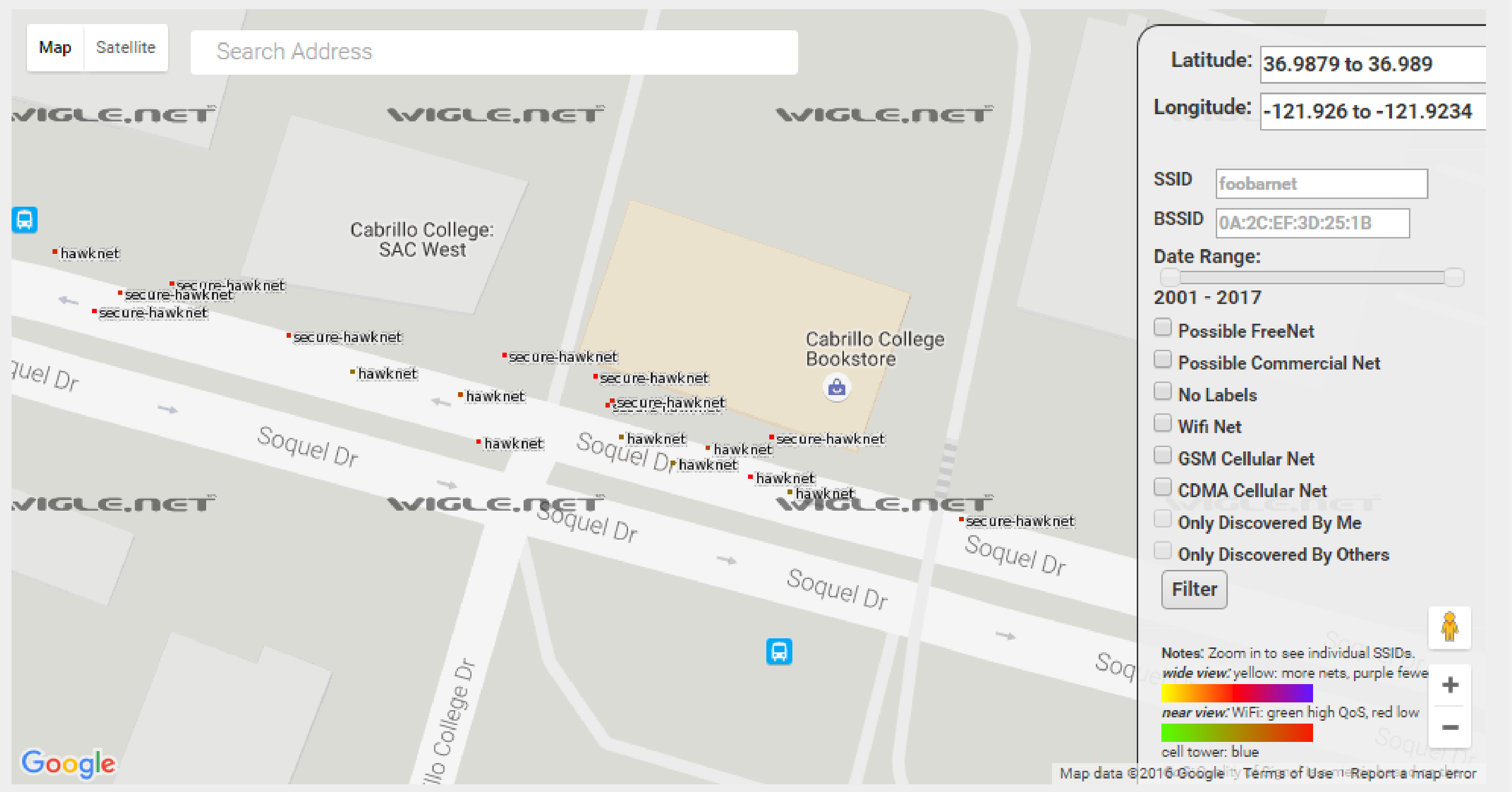
L-com® Global Connectivity

For more information, visit us at www.L-com.com or call 1-800-343-1455

http://www.l-com.com/content/802.11-Wireless-Standards.pdf

WIGLE.NET

Zooming in to see specific SSID's



Latitude: 36.9879 to 36.989

Longitude: -121.926 to -121.9234

SSID foobarnet

BSSID 0A:2C:EF:3D:25:1B

Date Range:

2001 - 2017

- □ Possible FreeNet
- □ Possible Commercial Net
- □ No Labels
- □ Wifi Net
- □ GSM Cellular Net
- □ CDMA Cellular Net
- □ Only Discovered By Me
- □ Only Discovered By Others

Filter

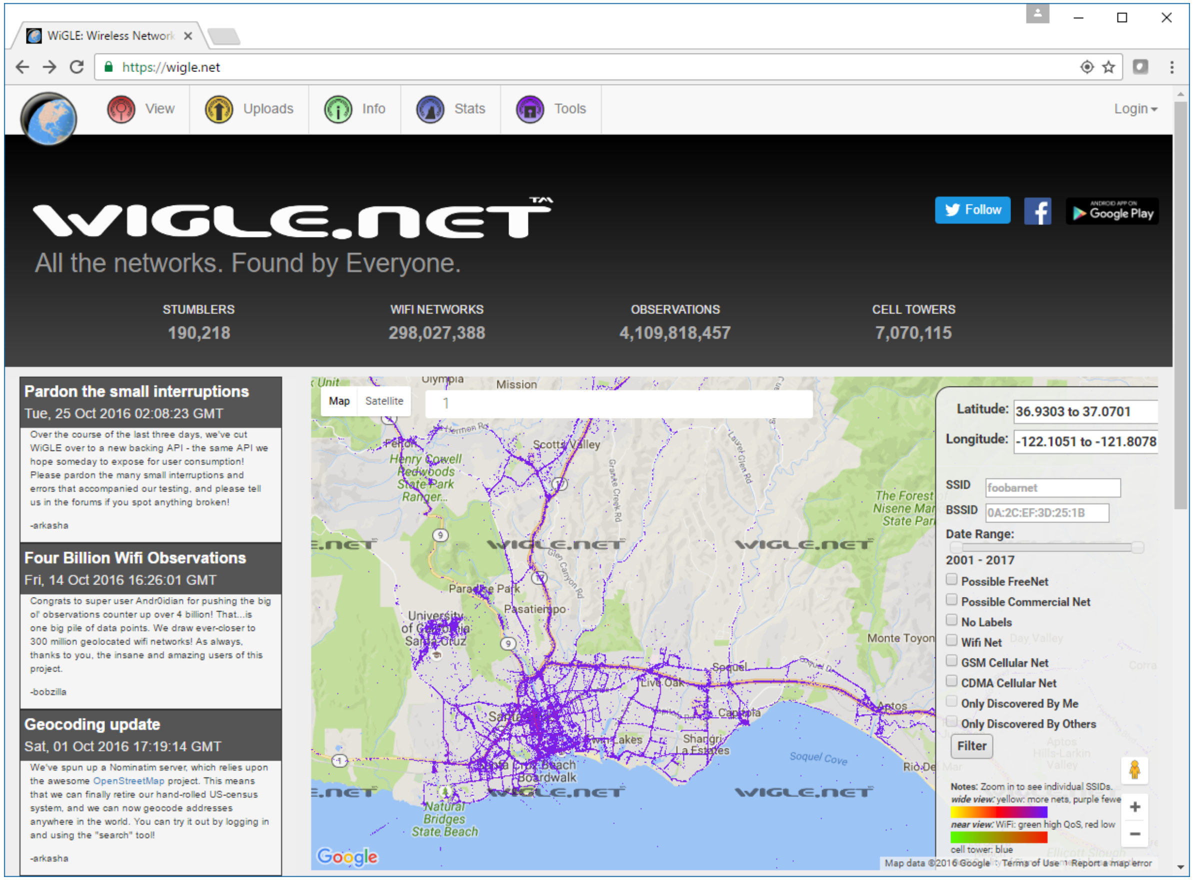
Notes: Zoom in to see individual SSIDs.
wide view: yellow: more nets, purple fewe
near view: WiFi: green high QoS, red low
cell tower: blue

Map data ©2016 Google Terms of Use Report a map error

https://wigle.net/

WIGLE.NET

Access Points on Google Maps



WIGLE.NET

All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	OBSERVATIONS	CELL TOWERS
190,218	298,027,388	4,109,818,457	7,070,115

Pardon the small interruptions

Tue, 25 Oct 2016 02:08:23 GMT

Over the course of the last three days, we've cut WiGLE over to a new backing API - the same API we hope someday to expose for user consumption! Please pardon the many small interruptions and errors that accompanied our testing, and please tell us in the forums if you spot anything broken!

-arkasha

Four Billion Wifi Observations

Fri, 14 Oct 2016 16:26:01 GMT

Congrats to super user Andr0idian for pushing the big ol' observations counter up over 4 billion! That...is one big pile of data points. We draw ever-closer to 300 million geolocated wifi networks! As always, thanks to you, the insane and amazing users of this project.

-bobzilla

Geocoding update

Sat, 01 Oct 2016 17:19:14 GMT

We've spun up a Nominatim server, which relies upon the awesome OpenStreetMap project. This means that we can finally retire our hand-rolled US-census system, and we can now geocode addresses anywhere in the world. You can try it out by logging in and using the "search" tool!

-arkasha

Latitude: 36.9303 to 37.0701

Longitude: -122.1051 to -121.8078

SSID foobarnet

BSSID 0A:2C:EF:3D:25:1B

Date Range:

2001 - 2017

□ Possible FreeNet

□ Possible Commercial Net

□ No Labels

□ Wifi Net

□ GSM Cellular Net

□ CDMA Cellular Net

□ Only Discovered By Me

□ Only Discovered By Others

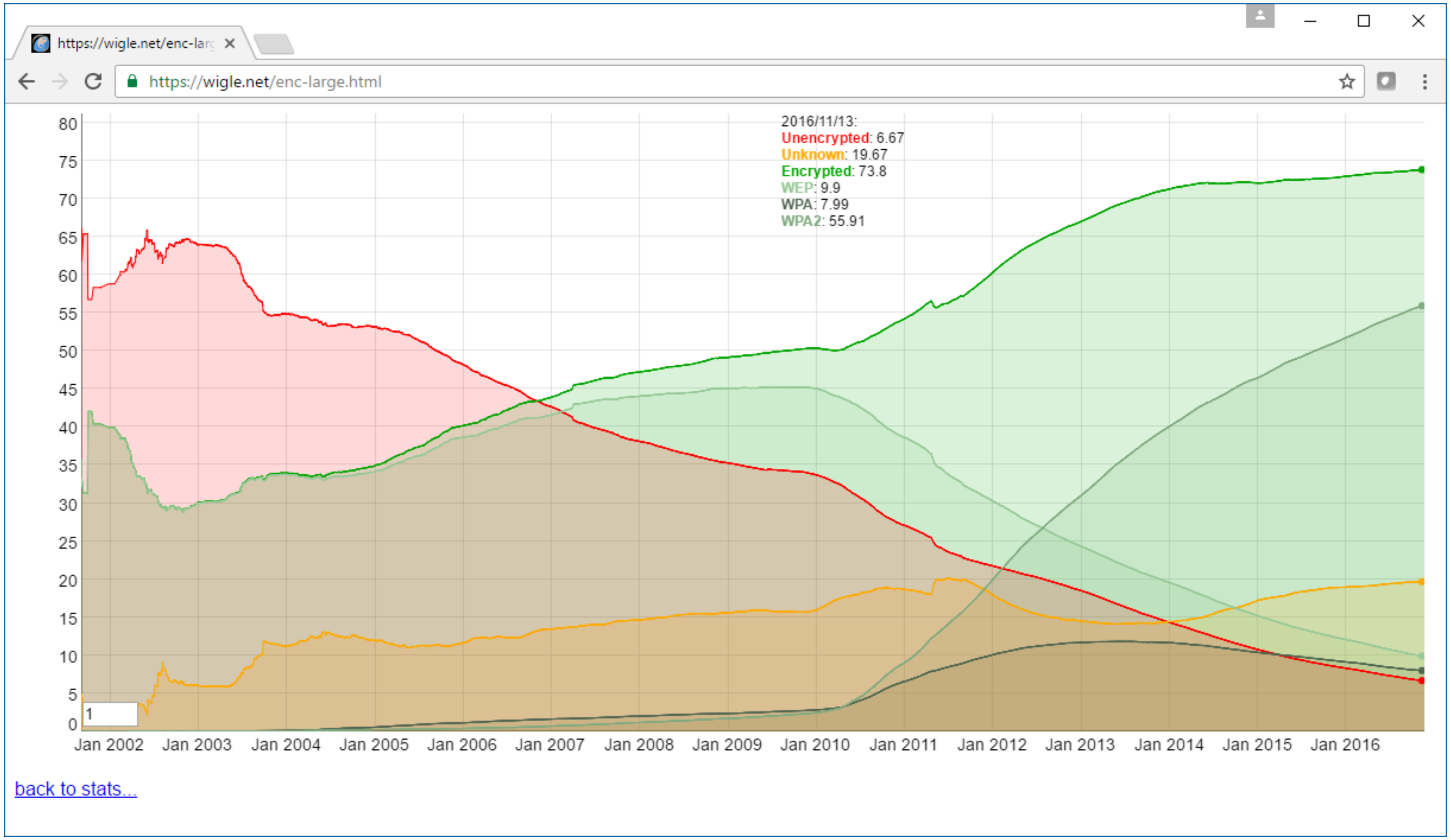
Notes: Zoom in to see individual SSIDs.
wide view: yellow: more nets, purple fewe
near view: WiFi: green high QoS, red low
cell tower: blue

Map data ©2016 Google Terms of Use Report a map error

https://wigle.net/

WIGLE.NET

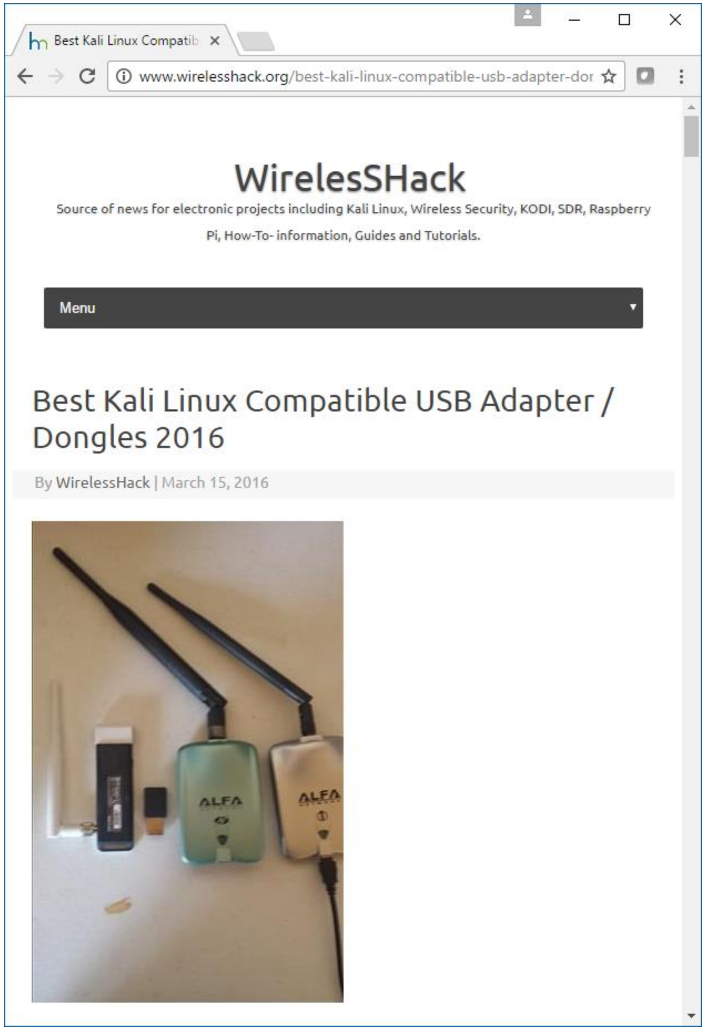
Full screen view of Wi-Fi Encryption Over Time



back to stats...

https://wigle.net/

Special Adapters and Utilities for Hacking


Best Kali Linux Compatib
www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dor
Menu
ALFA
ALFA

WirelesSHack

Source of news for electronic projects including Kali Linux, Wireless Security, KODI, SDR, Raspberry Pi, How-To- information, Guides and Tutorials.

Best Kali Linux Compatible USB Adapter / Dongles 2016

By WirelessHack | March 15, 2016

http://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles-2016.html

What Makes a Kali Linux USB Adapter Compatible?
The chipset and drivers written for a card is what makes a dongle compatible with Kali.

To do wireless Penetration Testing a card must be able to go into monitor mode and do packet injections most cards cant do this.

There are known chipsets that will work with Kali and Pen testing.

Most Popular Kali Linux Chipsets.
Atheros AR9271
Ralink RT3070
Ralink RT3572

For this lesson I used:

- A MacBook Pro with MacPorts and Aircrack-NG.
- The EH-Kali-xx VM in the EH Pod (Aircrack-NG already installed).

+ MacPorts + AIRCRACK-NG

https://www.macports.org/

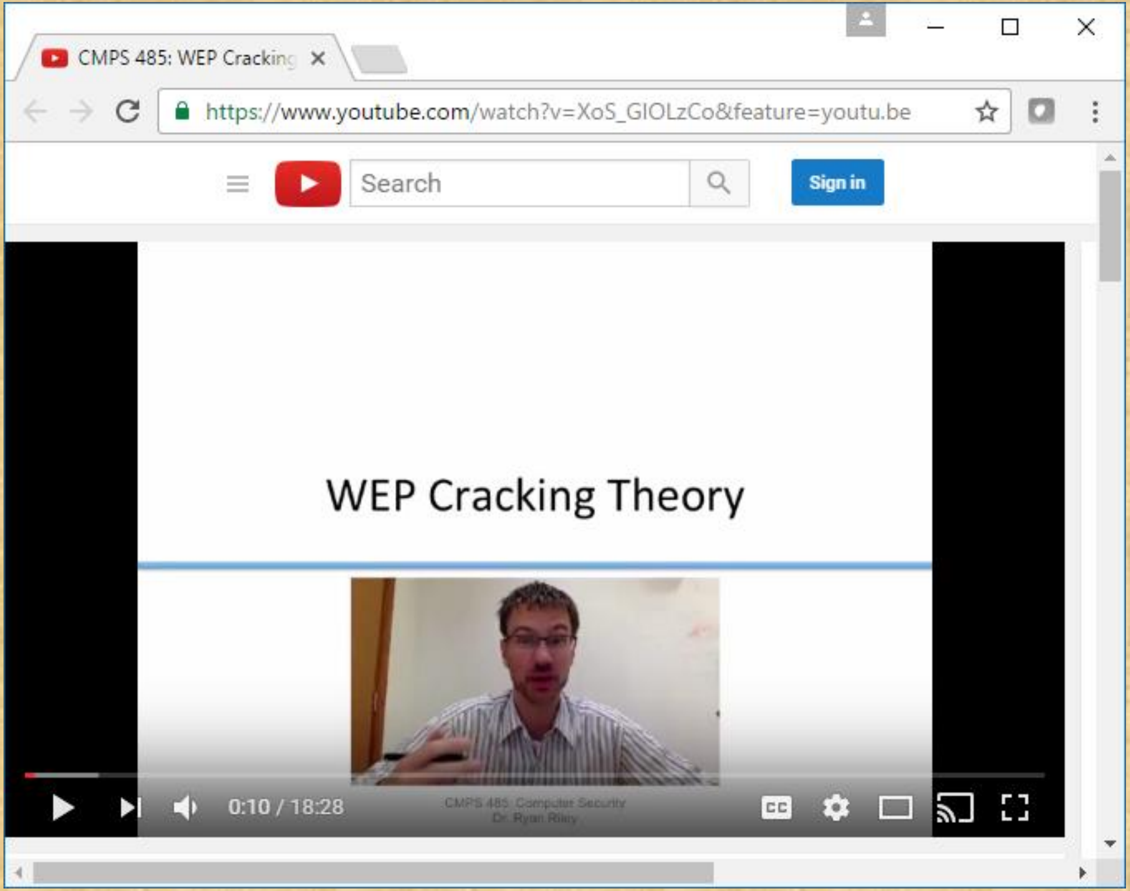
http://www.aircrack-ng.org/

Hacking WEP

Wired Equivalent Privacy (WEP)

- Defined in the 802.11b standard.
- Encrypts data on a wireless network.
- Uses the insecure RC4 stream cipher.
- WEP can be cracked in minutes.

https://www.youtube.com/watch?v=XoS_GIOLzCo&feature=youtu.be


CMPS 485: WEP Cracking
https://www.youtube.com/watch?v=XoS_GIOLzCo&feature=youtu.be
Search
Sign in
WEP Cracking Theory
0:10 / 18:28
CMPS 485: Computer Security
Dr. Ryan Riley

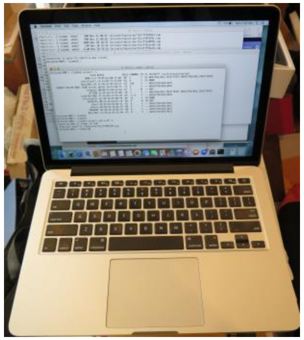
Ryan Riley had created an excellent video on how WEP and WEP cracking works.

If you get a chance watch the whole video. We will just look a portion tonight.

Start at 02:41... stop at 10:30

WEP Cracking with a Linksys WAP54G Access Point

BSSID
= Basic Service Set Identifier
= AP Mac Address
= 00:06:25:4b:21:b4

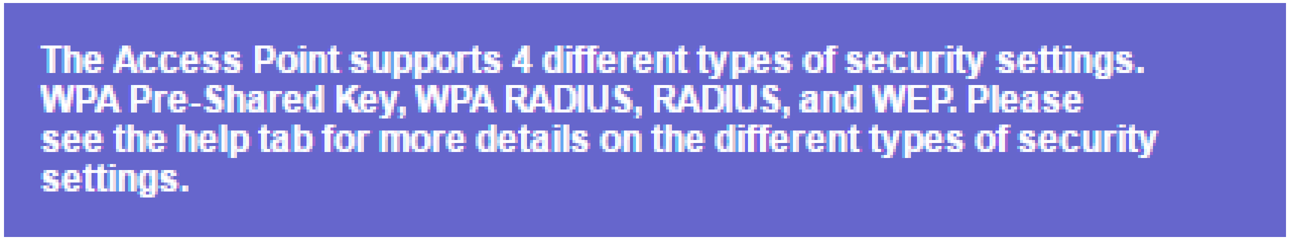


STA
= Station
= MacBook Pro

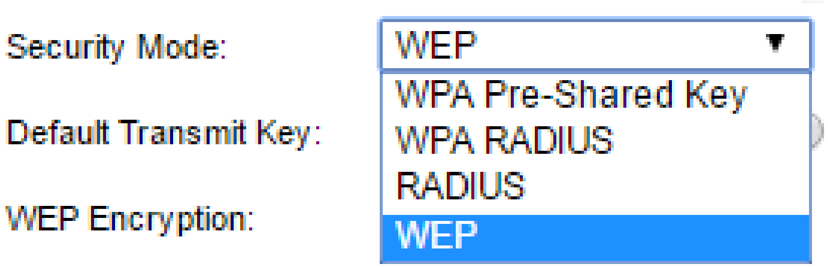
STA
= Station
= Win 10 PC

SSID
= Service Set Identifier
= Name of the network
= linkysys

Linksys WAP54G



The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.



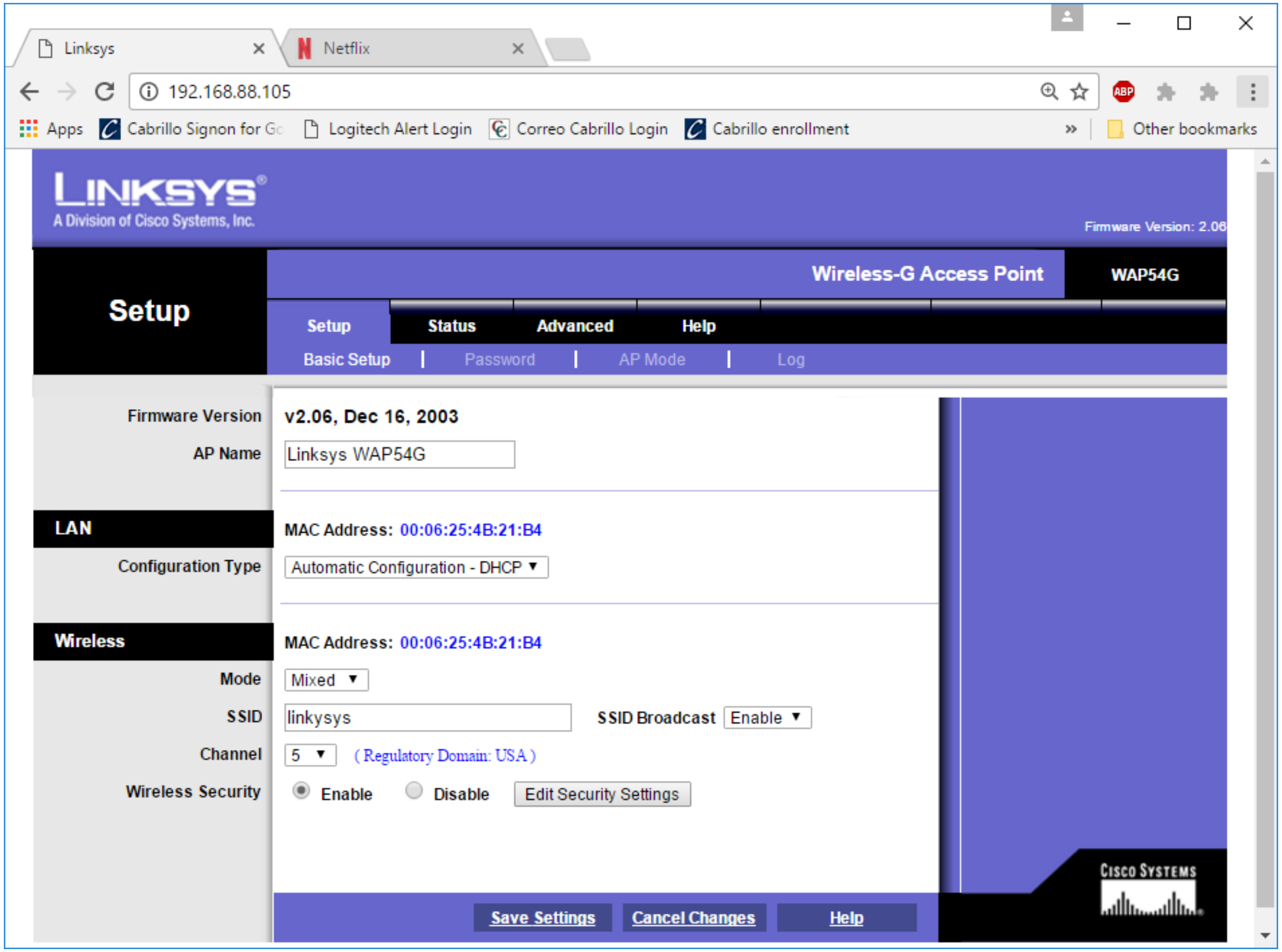
Security Mode: WEP ▼

Default Transmit Key:

WEP Encryption:

For this example we will use WEP (Wired Equivalent Privacy)

Linksys WAP54G



Firmware Version: v2.06, Dec 16, 2003

AP Name: Linksys WAP54G

LAN

MAC Address: 00:06:25:4B:21:B4

Configuration Type: Automatic Configuration - DHCP

Wireless

MAC Address: 00:06:25:4B:21:B4

Mode: Mixed

SSID: linkysys

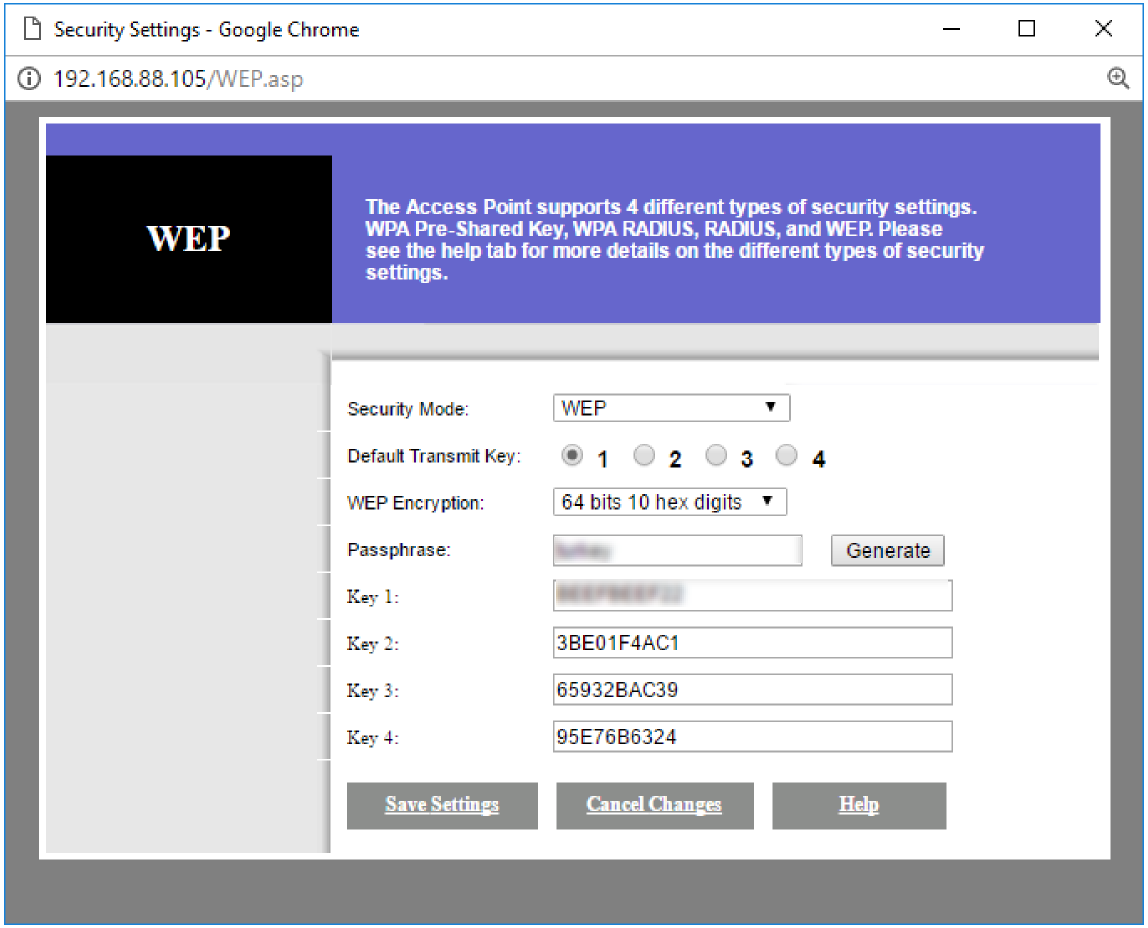
SSID Broadcast: Enable

Channel: 5 (Regulatory Domain: USA)

Wireless Security: ● Enable ○ Disable Edit Security Settings

Using Mixed Mode (B and G), Channel 5, and Wireless Security (WEP)

Linksys WAP54G



Security Settings - Google Chrome

192.168.88.105/WEP.asp

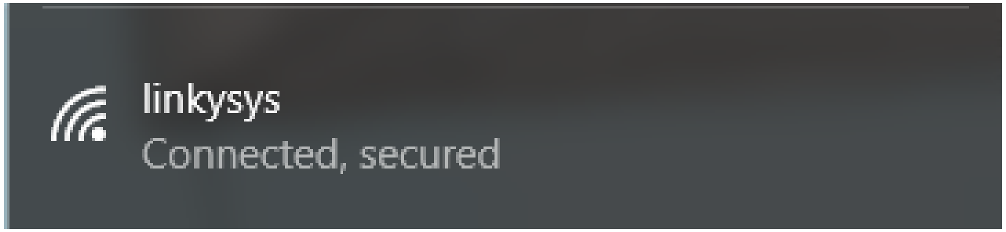
WEP

The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode:	WEP ▼
Default Transmit Key:	● 1 ○ 2 ○ 3 ○ 4
WEP Encryption:	64 bits 10 hex digits ▼
Passphrase:	[redacted] Generate
Key 1:	[redacted]
Key 2:	3BE01F4AC1
Key 3:	65932BAC39
Key 4:	95E76B6324

Generate a key from a pass phrase and use Key 1 on each station

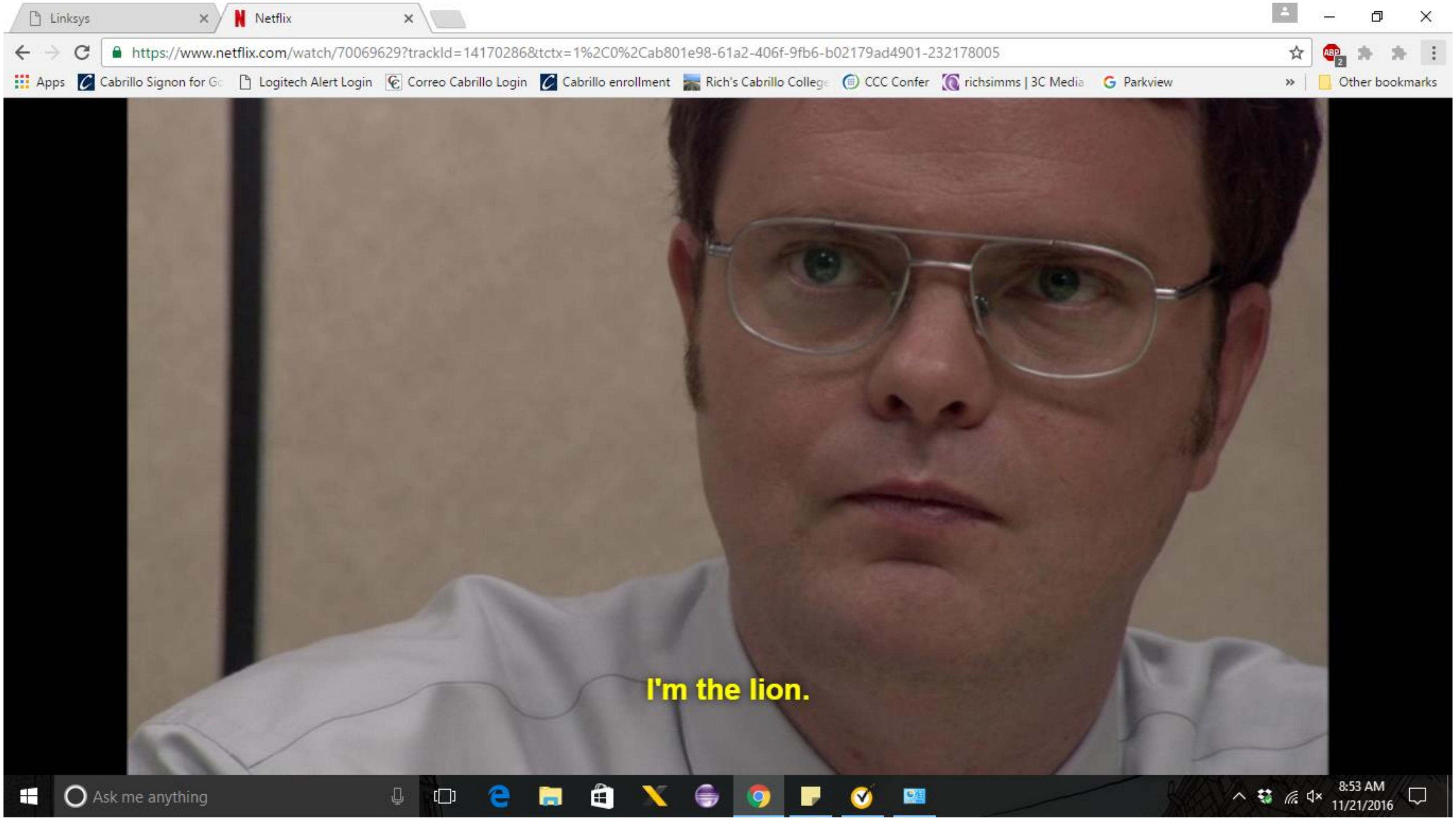
Windows 10 PC View



linkysys
Connected, secured

SSID:	linkysys
Protocol:	802.11g
Security type:	Open
Network band:	2.4 GHz
Network channel:	5
IPv4 address:	192.168.88.112
Manufacturer:	Intel Corporation
Description:	Intel(R) Centrino(R) Wireless-N 1030
Driver version:	15.11.0.7
Physical address (MAC):	4C-EB-42-85-71-B8

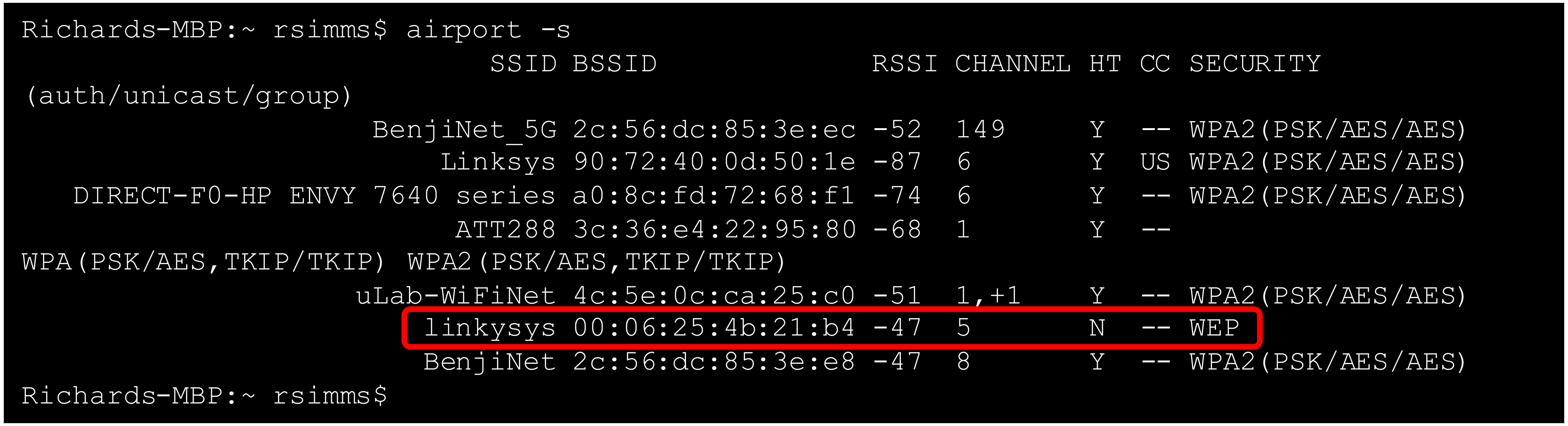
Connected to the linkysys SSID network



Watching an Office episode on Netflix so we have some encrypted packets to sniff.

Sniffing using MacBook Pro

airport -s

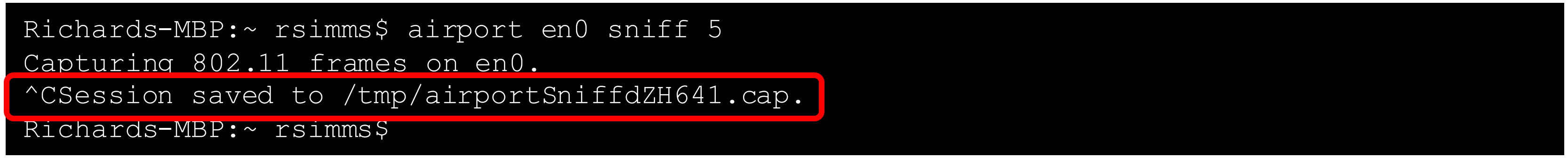


```
Richards-MBP:~ rsimms$ airport -s
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY
(auth/unicast/group)
                     BenjiNet_5G 2c:56:dc:85:3e:ec -52  149     Y  -- WPA2(PSK/AES/AES)
                         Linksys 90:72:40:0d:50:1e -87  6       Y  US WPA2(PSK/AES/AES)
   DIRECT-F0-HP ENVY 7640 series a0:8c:fd:72:68:f1 -74  6       Y  -- WPA2(PSK/AES/AES)
                          ATT288 3c:36:e4:22:95:80 -68  1       Y  --
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                    uLab-WiFiNet 4c:5e:0c:ca:25:c0 -51  1,+1    Y  -- WPA2(PSK/AES/AES)
                        linkysys 00:06:25:4b:21:b4 -47  5       N  -- WEP
                        BenjiNet 2c:56:dc:85:3e:e8 -47  8       Y  -- WPA2(PSK/AES/AES)
Richards-MBP:~ rsimms$
```

On a MacBook Pro, the built in airport command with an -s option will scan all available WiFi networks.

Sniffing using MacBook Pro

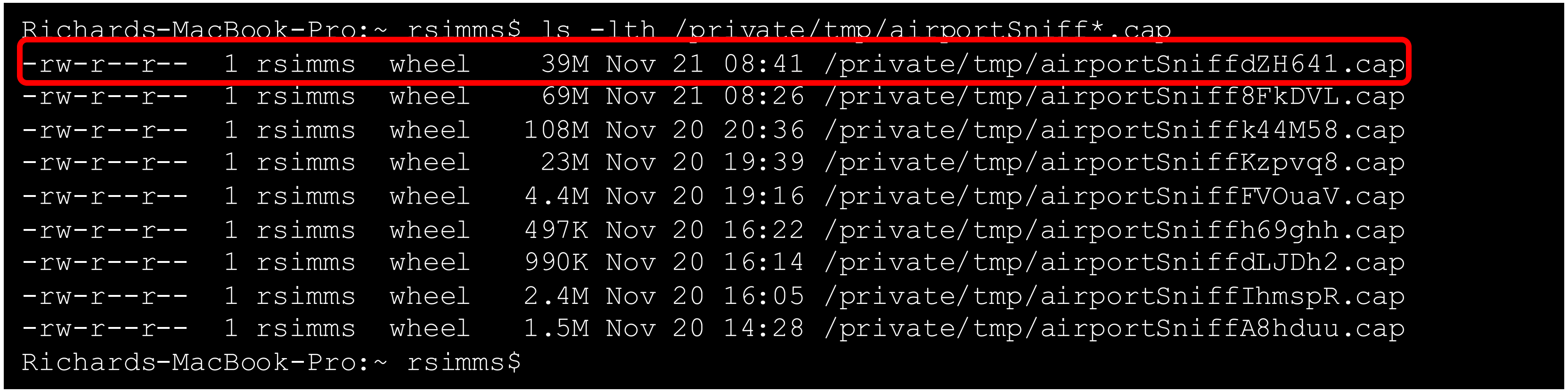
airport en0 sniff 5



```
Richards-MBP:~ rsimms$ airport en0 sniff 5
Capturing 802.11 frames on en0.
^CSession saved to /tmp/airportSniffdZH641.cap.
Richards-MBP:~ rsimms$
```

Let's start sniffing the channel used by the access point for the SSID linkysys. Use control-C to stop the capture.

ls -lth /private/tmp/airportSniff*.cap



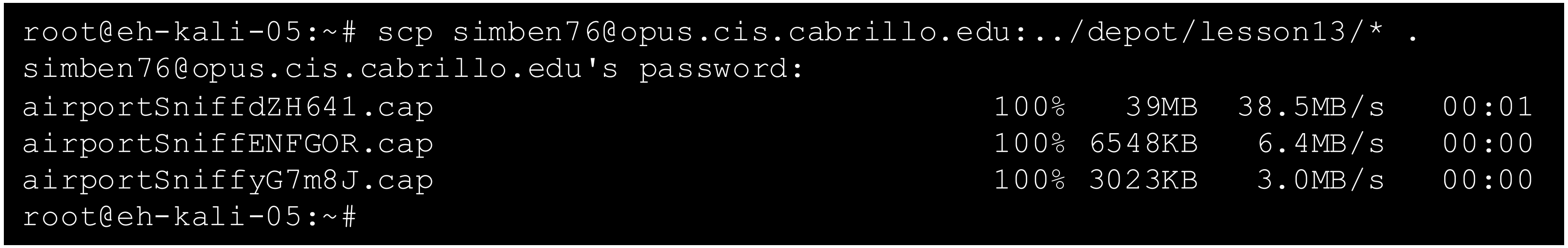
```
Richards-MacBook-Pro:~ rsimms$ ls -lth /private/tmp/airportSniff*.cap
-rw-r--r--  1 rsimms  wheel    39M Nov 21 08:41 /private/tmp/airportSniffdZH641.cap
-rw-r--r--  1 rsimms  wheel    69M Nov 21 08:26 /private/tmp/airportSniff8FkDVL.cap
-rw-r--r--  1 rsimms  wheel   108M Nov 20 20:36 /private/tmp/airportSniffk44M58.cap
-rw-r--r--  1 rsimms  wheel    23M Nov 20 19:39 /private/tmp/airportSniffKzpvq8.cap
-rw-r--r--  1 rsimms  wheel   4.4M Nov 20 19:16 /private/tmp/airportSniffFVOuaV.cap
-rw-r--r--  1 rsimms  wheel   497K Nov 20 16:22 /private/tmp/airportSniffh69ghh.cap
-rw-r--r--  1 rsimms  wheel   990K Nov 20 16:14 /private/tmp/airportSniffdLJDh2.cap
-rw-r--r--  1 rsimms  wheel   2.4M Nov 20 16:05 /private/tmp/airportSniffIhmspR.cap
-rw-r--r--  1 rsimms  wheel   1.5M Nov 20 14:28 /private/tmp/airportSniffA8hduu.cap
Richards-MacBook-Pro:~ rsimms$
```

The packets are captured and dumped into a new file in the /private/tmp directory with any previous captures.

Captures transferred to Kali

WEP Cracking

`scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .`



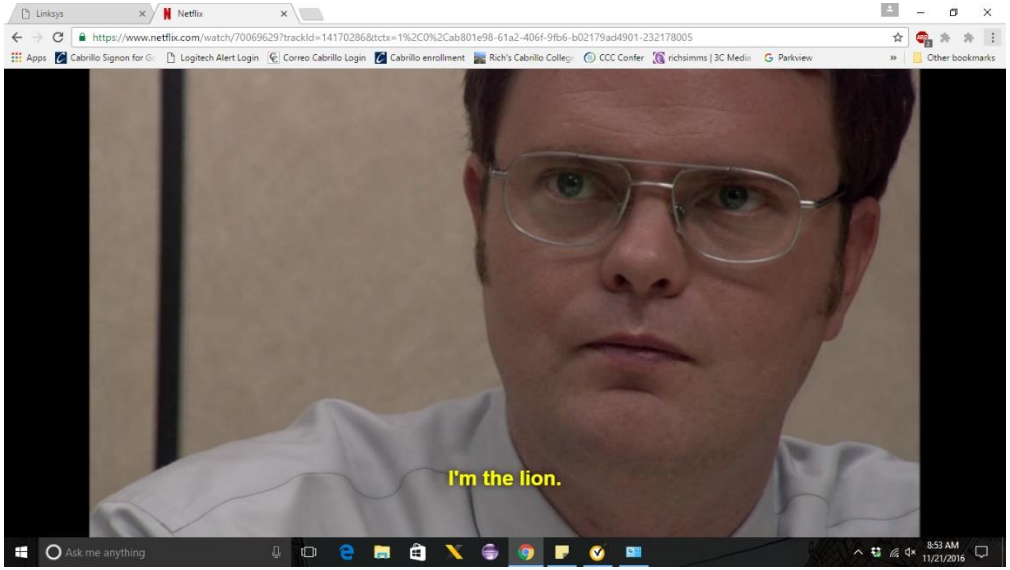
```
root@eh-kali-05:~# scp simben76@opus.cis.cabrillo.edu:../depot/lesson13/* .
simben76@opus.cis.cabrillo.edu's password:
airportSniffdZH641.cap                                100%   39MB  38.5MB/s   00:01
airportSniffENFGOR.cap                                100% 6548KB   6.4MB/s   00:00
airportSniffyG7m8J.cap                                100% 3023KB   3.0MB/s   00:00
root@eh-kali-05:~#
```

Copying the packet capture files to the EH-Kali-XX VM

Capture

dZH641

airportSniffdZH641.cap



This capture was done while watching a portion of an Office episode on Netflix

WEP Cracking

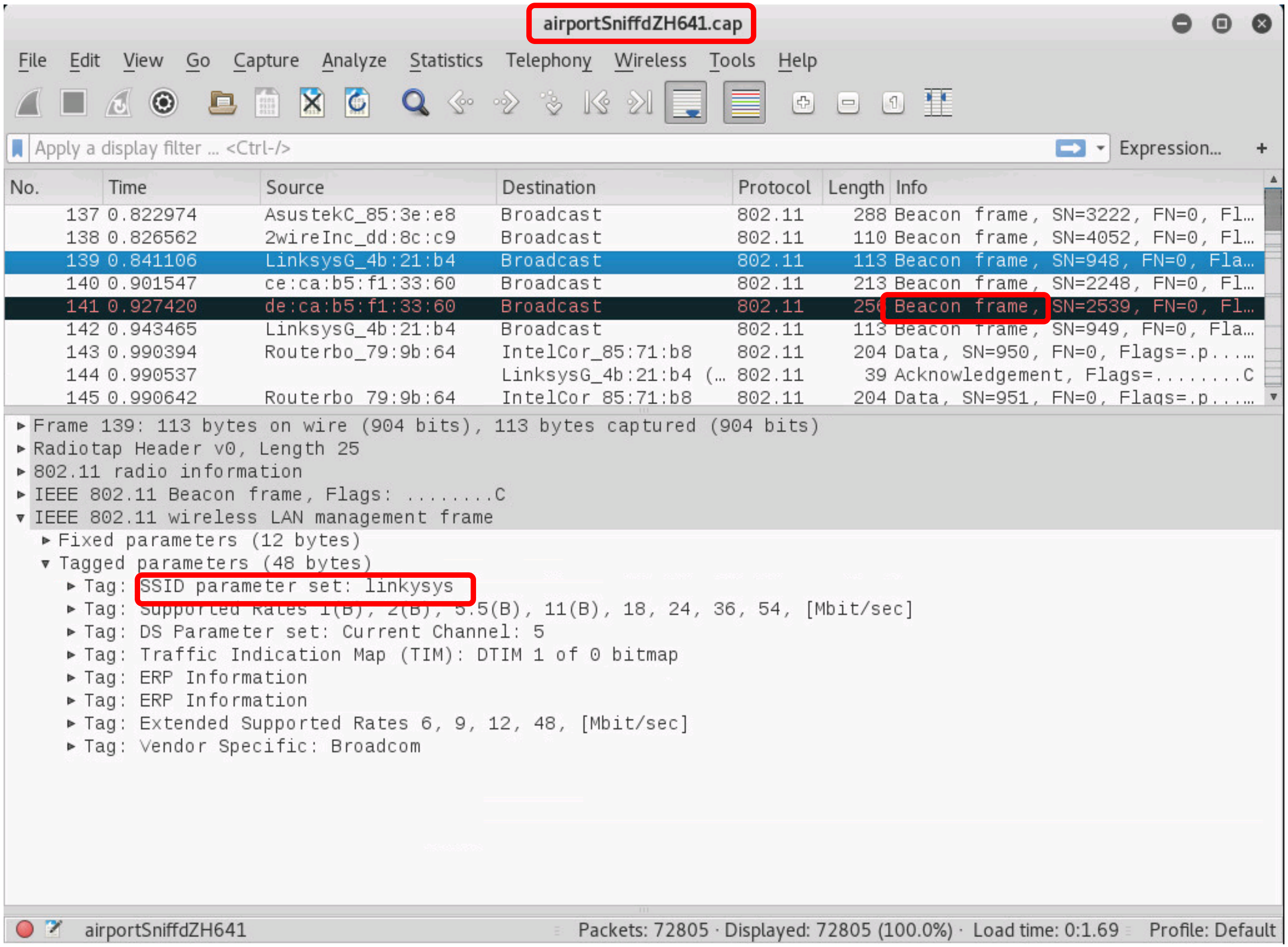
ls -l airportSniffdZH641.cap

```
root@eh-kali-05:~# ls -l airportSniffdZH641.cap
-rw-r--r-- 1 root root 40401050 Nov 21 12:31 airportSniffdZH641.cap
root@eh-kali-05:~#
```

file airportSniffdZH641.cap

```
root@eh-kali-05:~# file airportSniffdZH641.cap
airportSniffdZH641.cap: tcpdump capture file (little-endian) - version 2.4 (802.11
with radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

WEP Cracking


airportSniffdZH641.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source              Destination          Protocol Length Info
  137 0.822974  AsustekC_85:3e:e8   Broadcast            802.11    288 Beacon frame, SN=3222, FN=0, Fl…
  138 0.826562  2wireInc_dd:8c:c9   Broadcast            802.11    110 Beacon frame, SN=4052, FN=0, Fl…
  139 0.841106  LinksysG_4b:21:b4   Broadcast            802.11    113 Beacon frame, SN=948, FN=0, Fla…
  140 0.901547  ce:ca:b5:f1:33:60   Broadcast            802.11    213 Beacon frame, SN=2248, FN=0, Fl…
  141 0.927420  de:ca:b5:f1:33:60   Broadcast            802.11    256 Beacon frame, SN=2539, FN=0, Fl…
  142 0.943465  LinksysG_4b:21:b4   Broadcast            802.11    113 Beacon frame, SN=949, FN=0, Fla…
  143 0.990394  Routerbo_79:9b:64   IntelCor_85:71:b8    802.11    204 Data, SN=950, FN=0, Flags=.p....…
  144 0.990537                      LinksysG_4b:21:b4 (… 802.11     39 Acknowledgement, Flags=........C
  145 0.990642  Routerbo_79:9b:64   IntelCor_85:71:b8    802.11    204 Data, SN=951, FN=0, Flags=.p....…
```

```
▸ Frame 139: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (48 bytes)
    ▸ Tag: SSID parameter set: linksys
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 5
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: Vendor Specific: Broadcom
```

airportSniffdZH641 Packets: 72805 · Displayed: 72805 (100.0%) · Load time: 0:1.69 Profile: Default

We can see one of the beacon frames from the Linksys WAP54G

Activity

As root, on your EH-Kali-XX VM:

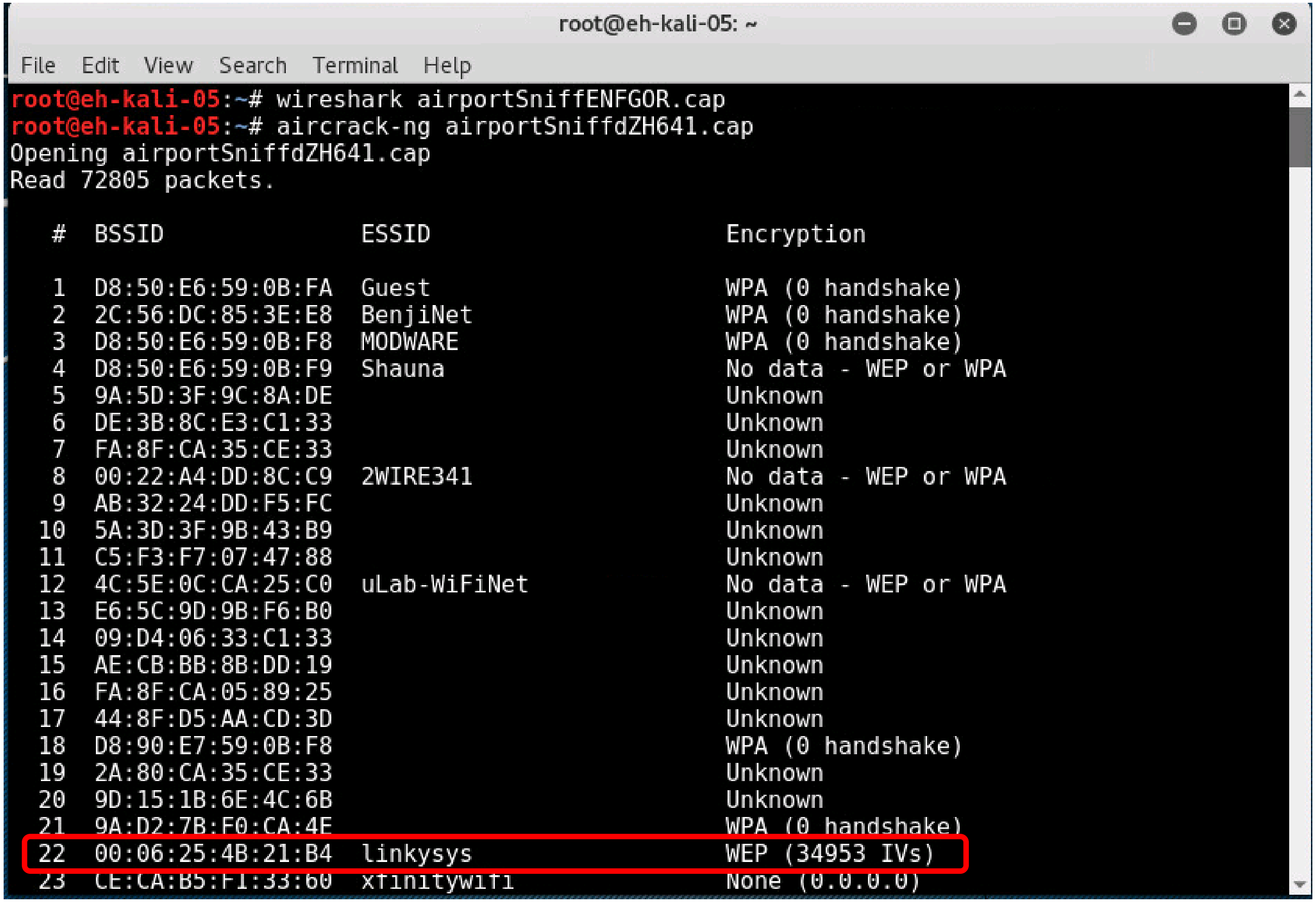
1) **scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .**

2) Run wireshark and look at the airportSniffdZH641.cap file.

3) Find some more Beacon frames. What other SSID's can you discover in this capture?

Write your SSID's in the chat window

aircrack-ng airportSniffdZH641.cap



```
root@eh-kali-05:~# wireshark airportSniffENFGOR.cap
root@eh-kali-05:~# aircrack-ng airportSniffdZH641.cap
Opening airportSniffdZH641.cap
Read 72805 packets.

   #  BSSID              ESSID                     Encryption

   1  D8:50:E6:59:0B:FA  Guest                     WPA (0 handshake)
   2  2C:56:DC:85:3E:E8  BenjiNet                  WPA (0 handshake)
   3  D8:50:E6:59:0B:F8  MODWARE                   WPA (0 handshake)
   4  D8:50:E6:59:0B:F9  Shauna                    No data - WEP or WPA
   5  9A:5D:3F:9C:8A:DE                            Unknown
   6  DE:3B:8C:E3:C1:33                            Unknown
   7  FA:8F:CA:35:CE:33                            Unknown
   8  00:22:A4:DD:8C:C9  2WIRE341                  No data - WEP or WPA
   9  AB:32:24:DD:F5:FC                            Unknown
  10  5A:3D:3F:9B:43:B9                            Unknown
  11  C5:F3:F7:07:47:88                            Unknown
  12  4C:5E:0C:CA:25:C0  uLab-WiFiNet              No data - WEP or WPA
  13  E6:5C:9D:9B:F6:B0                            Unknown
  14  09:D4:06:33:C1:33                            Unknown
  15  AE:CB:BB:8B:DD:19                            Unknown
  16  FA:8F:CA:05:89:25                            Unknown
  17  44:8F:D5:AA:CD:3D                            Unknown
  18  D8:90:E7:59:0B:F8                            WPA (0 handshake)
  19  2A:80:CA:35:CE:33                            Unknown
  20  9D:15:1B:6E:4C:6B                            Unknown
  21  9A:D2:7B:F0:CA:4E                            WPA (0 handshake)
  22  00:06:25:4B:21:B4  linkysys                  WEP (34953 IVs)
  23  CE:CA:B5:F1:33:60  xfinitywifi               None (0.0.0.0)
```

Using aircrack-ng to crack the WEP password

Activity

As root, on your EH-Kali-XX VM:

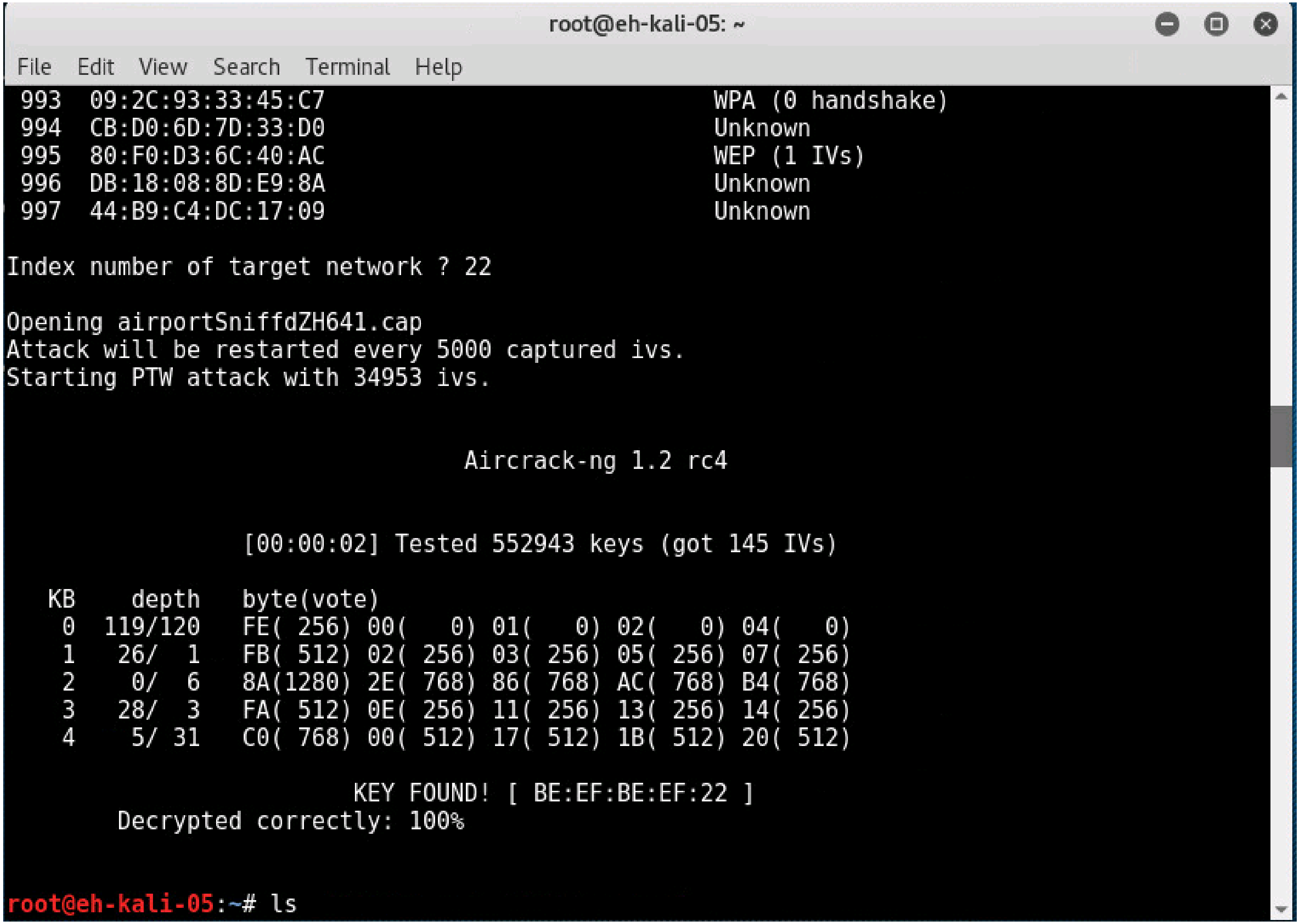
1. **scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .**

2. **aircrack-ng airportSniffdZH641.cap**

3. Select the "Linkysys" SSID

The one with the "y" (not Linksys)

What is the WEP password? Write your answer in the chat window



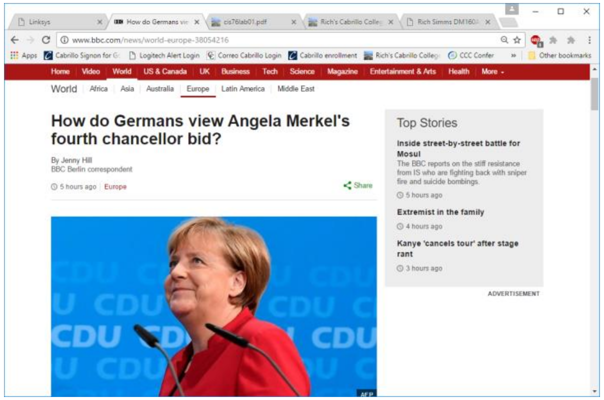
```
 993  09:2C:93:33:45:C7                          WPA (0 handshake)
 994  CB:D0:6D:7D:33:D0                          Unknown
 995  80:F0:D3:6C:40:AC                          WEP (1 IVs)
 996  DB:18:08:8D:E9:8A                          Unknown
 997  44:B9:C4:DC:17:09                          Unknown

Index number of target network ? 22

Opening airportSniffdZH641.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 34953 ivs.


                                 Aircrack-ng 1.2 rc4


                 [00:00:02] Tested 552943 keys (got 145 IVs)

   KB    depth   byte(vote)
    0  119/120   FE( 256) 00(   0) 01(   0) 02(   0) 04(   0)
    1   26/  1   FB( 512) 02( 256) 03( 256) 05( 256) 07( 256)
    2    0/  6   8A(1280) 2E( 768) 86( 768) AC( 768) B4( 768)
    3   28/  3   FA( 512) 0E( 256) 11( 256) 13( 256) 14( 256)
    4    5/ 31   C0( 768) 00( 512) 17( 512) 1B( 512) 20( 512)

                        KEY FOUND! [ BE:EF:BE:EF:22 ]
        Decrypted correctly: 100%


root@eh-kali-05:~# ls
```

We have the password now so next we will attempt to extract files from the traffic

Capture

ENFGOR

airportSniffENFGOR.cap



How do Germans view Angela Merkel's fourth chancellor bid?

By Jenny Hill
BBC Berlin correspondent

5 hours ago | Europe

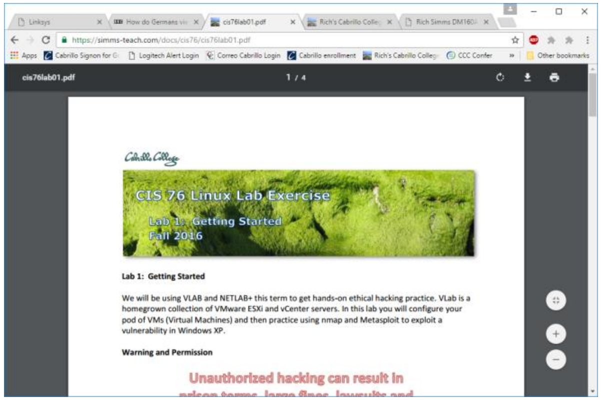
Top Stories

Inside street-by-street battle for Mosul
The BBC reports on the stiff resistance from IS who are fighting back with sniper fire and suicide bombings.
5 hours ago

Extremist in the family
4 hours ago

Kanye 'cancels tour' after stage rant
3 hours ago

http://www.bbc.com/news/world-europe-38054216



CIS 76 Linux Lab Exercise

Lab 1: Getting Started
Fall 2016

Lab 1: Getting Started

We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pod of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and

https://simms-teach.com/docs/cis76/cis76lab01.pdf

Getting files from packet captures

`ls -l airportSniffENFGOR.cap`

```
root@eh-kali-05:~# ls -l airportSniffENFGOR.cap
-rw-r--r-- 1 root root 6704919 Nov 21 12:31 airportSniffENFGOR.cap
```

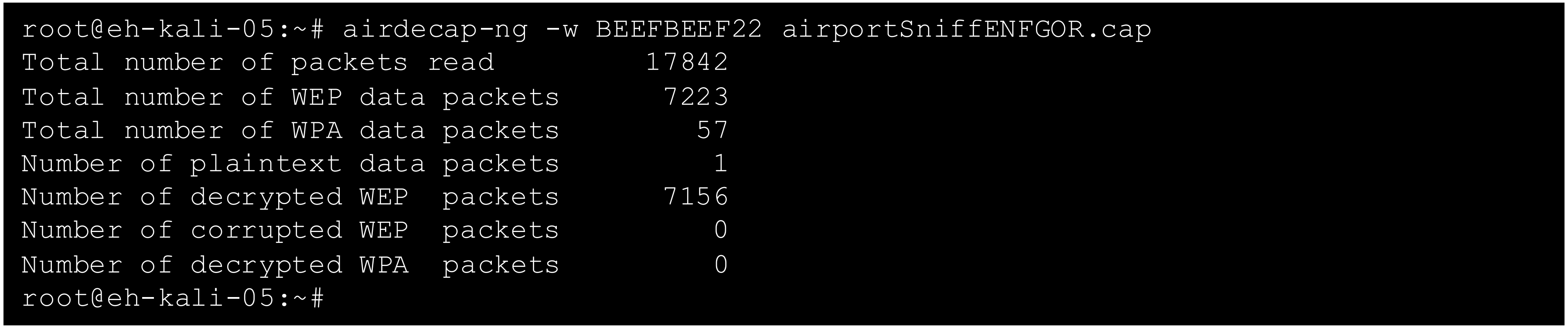
`file airportSniffENFGOR.cap`

```
root@eh-kali-05:~# file airportSniffENFGOR.cap
airportSniffENFGOR.cap: tcpdump capture file (little-endian) - version 2.4 (802.11 with
radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

Another packet capture file

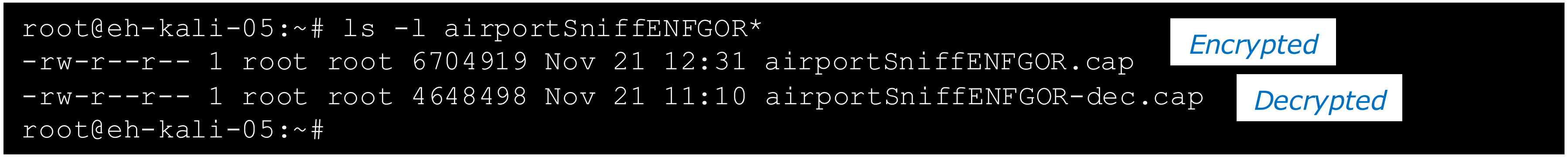
Getting files from packet captures

airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap



```
root@eh-kali-05:~# airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap
Total number of packets read          17842
Total number of WEP data packets       7223
Total number of WPA data packets         57
Number of plaintext data packets          1
Number of decrypted WEP  packets       7156
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets          0
root@eh-kali-05:~#
```

ls -l airportSniffENFGOR*



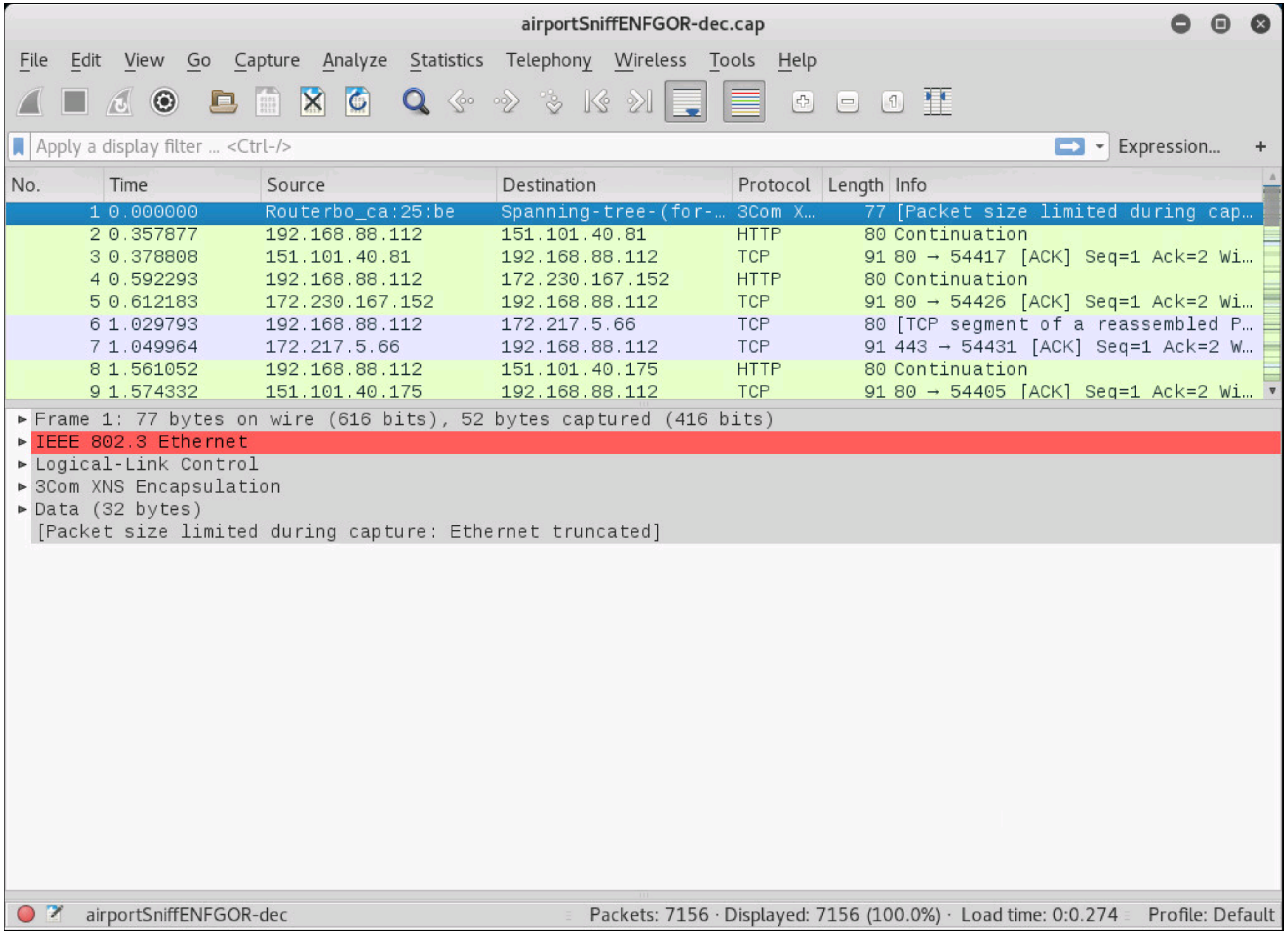
```
root@eh-kali-05:~# ls -l airportSniffENFGOR*
-rw-r--r-- 1 root root 6704919 Nov 21 12:31 airportSniffENFGOR.cap
-rw-r--r-- 1 root root 4648498 Nov 21 11:10 airportSniffENFGOR-dec.cap
root@eh-kali-05:~#
```

Encrypted

Decrypted

Decrypting the packet capture file

Getting files from packet captures

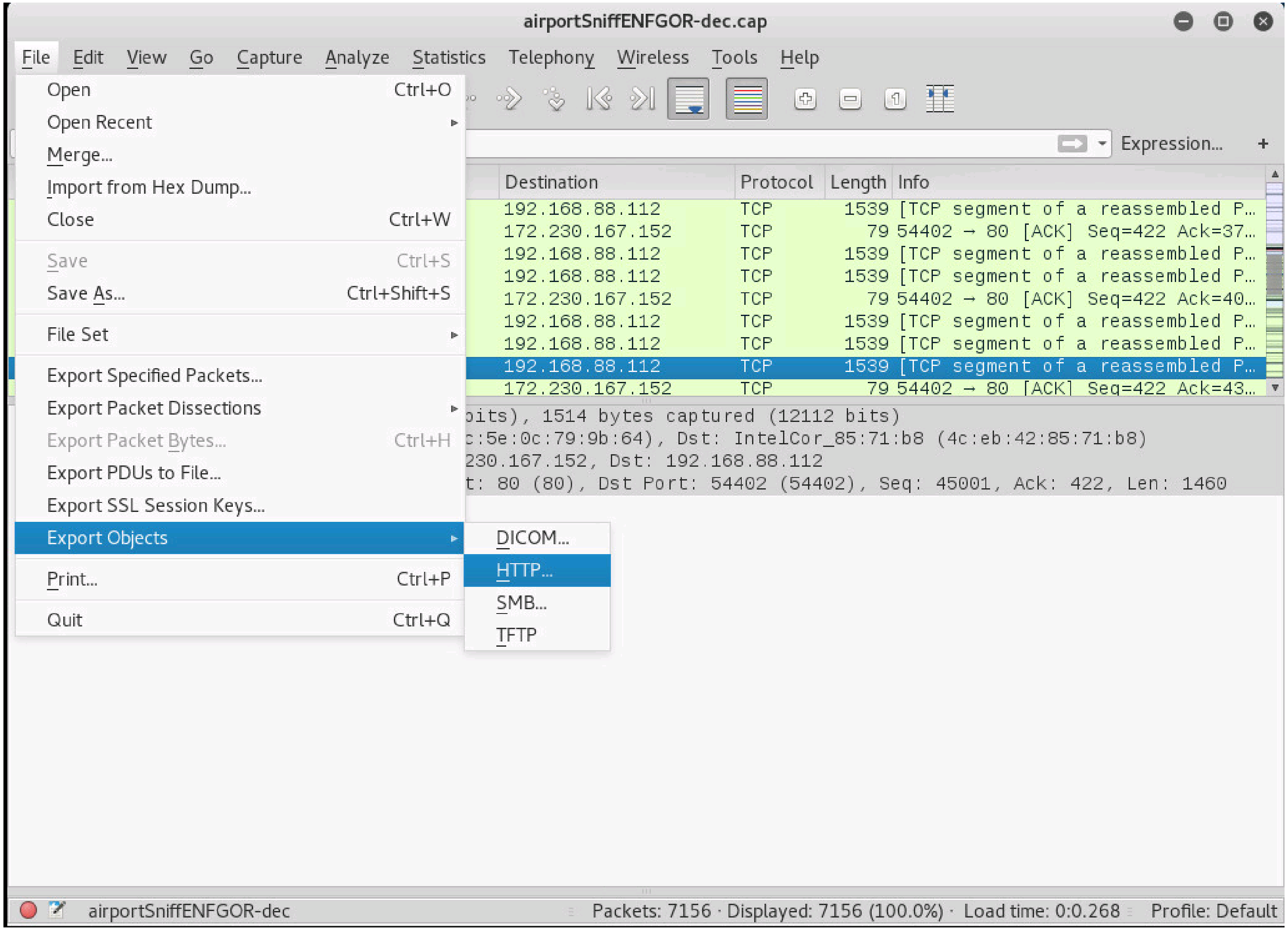


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Routerbo_ca:25:be	Spanning-tree-(for-…	3Com X…	77	[Packet size limited during cap…
2	0.357877	192.168.88.112	151.101.40.81	HTTP	80	Continuation
3	0.378808	151.101.40.81	192.168.88.112	TCP	91	80 → 54417 [ACK] Seq=1 Ack=2 Wi…
4	0.592293	192.168.88.112	172.230.167.152	HTTP	80	Continuation
5	0.612183	172.230.167.152	192.168.88.112	TCP	91	80 → 54426 [ACK] Seq=1 Ack=2 Wi…
6	1.029793	192.168.88.112	172.217.5.66	TCP	80	[TCP segment of a reassembled P…
7	1.049964	172.217.5.66	192.168.88.112	TCP	91	443 → 54431 [ACK] Seq=1 Ack=2 W…
8	1.561052	192.168.88.112	151.101.40.175	HTTP	80	Continuation
9	1.574332	151.101.40.175	192.168.88.112	TCP	91	80 → 54405 [ACK] Seq=1 Ack=2 Wi…

```
▸ Frame 1: 77 bytes on wire (616 bits), 52 bytes captured (416 bits)
▸ IEEE 802.3 Ethernet
▸ Logical-Link Control
▸ 3Com XNS Encapsulation
▸ Data (32 bytes)
  [Packet size limited during capture: Ethernet truncated]
```

airportSniffENFGOR-dec · Packets: 7156 · Displayed: 7156 (100.0%) · Load time: 0:0.274 · Profile: Default

We see traditional traffic now in the decrypted capture



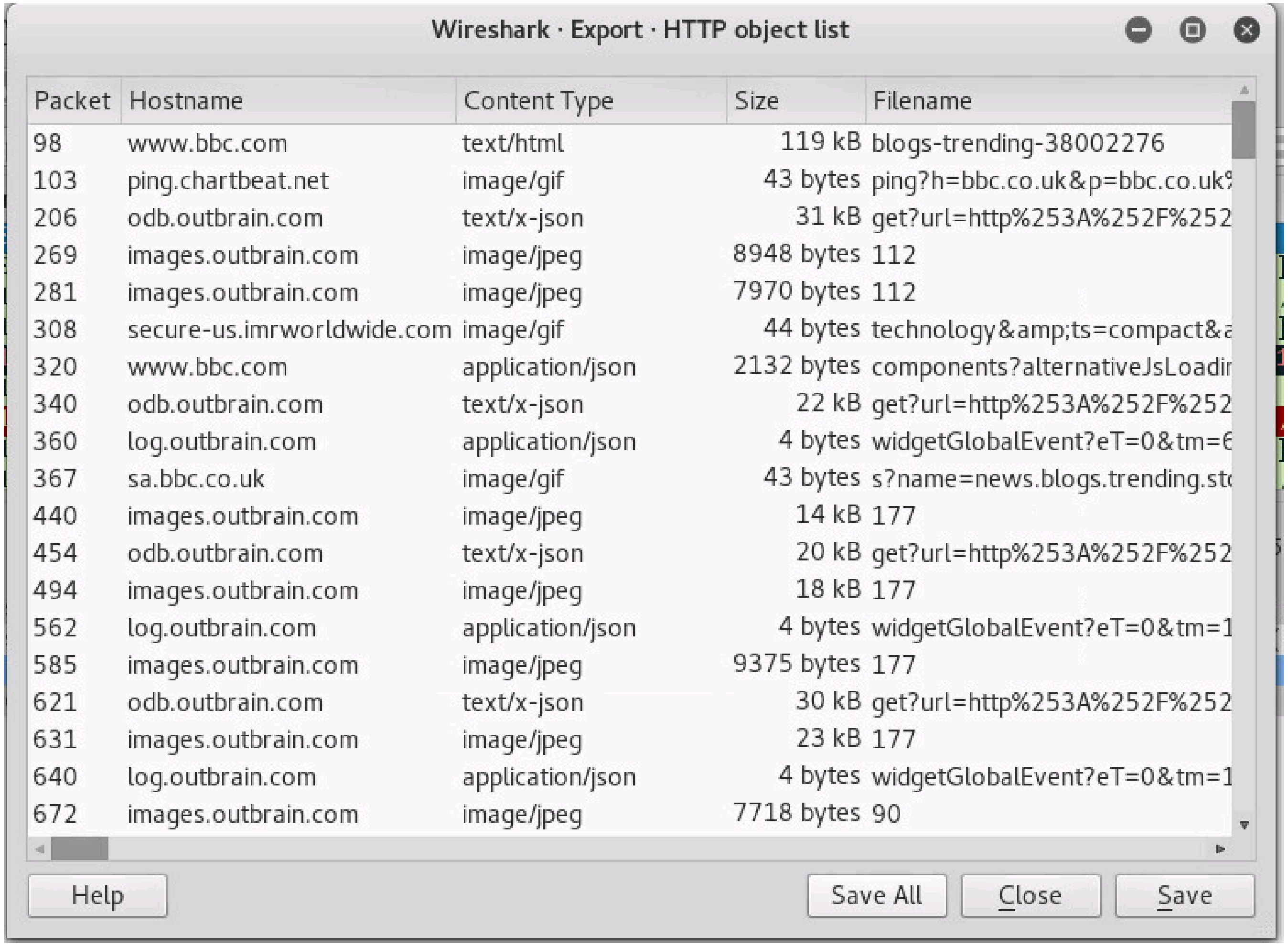
```
Destination        Protocol  Length  Info
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
172.230.167.152    TCP         79 54402 → 80 [ACK] Seq=422 Ack=37…
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
172.230.167.152    TCP         79 54402 → 80 [ACK] Seq=422 Ack=40…
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
192.168.88.112     TCP       1539 [TCP segment of a reassembled P…
172.230.167.152    TCP         79 54402 → 80 [ACK] Seq=422 Ack=43…
```

```
bits), 1514 bytes captured (12112 bits)
c:5e:0c:79:9b:64), Dst: IntelCor_85:71:b8 (4c:eb:42:85:71:b8)
230.167.152, Dst: 192.168.88.112
t: 80 (80), Dst Port: 54402 (54402), Seq: 45001, Ack: 422, Len: 1460
```

airportSniffENFGOR-dec   Packets: 7156 · Displayed: 7156 (100.0%) · Load time: 0:0.268   Profile: Default

File > Export Objects > HTTP

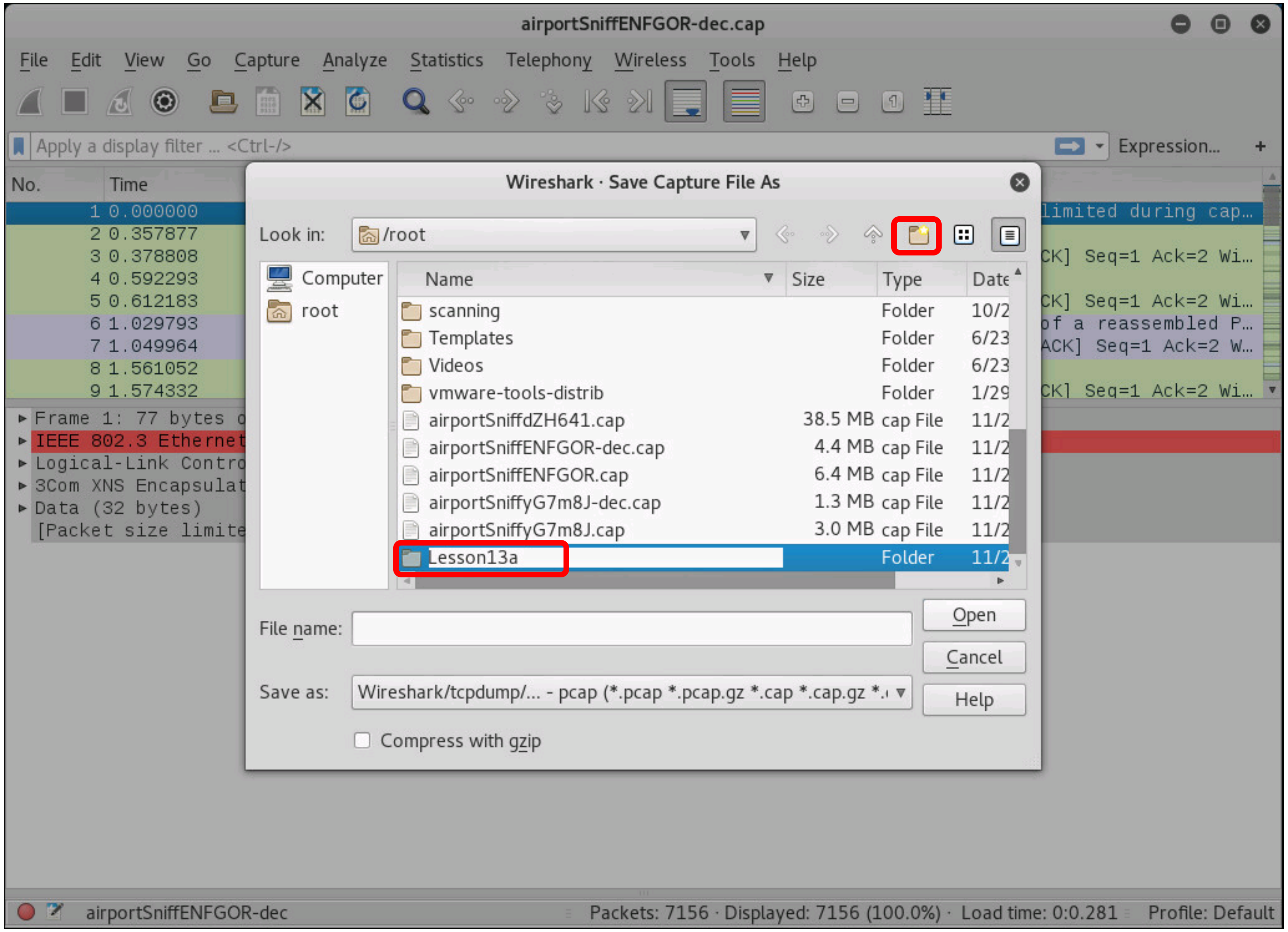
Getting files from packet captures



Packet	Hostname	Content Type	Size	Filename
98	www.bbc.com	text/html	119 kB	blogs-trending-38002276
103	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%
206	odb.outbrain.com	text/x-json	31 kB	get?url=http%253A%252F%252
269	images.outbrain.com	image/jpeg	8948 bytes	112
281	images.outbrain.com	image/jpeg	7970 bytes	112
308	secure-us.imrworldwide.com	image/gif	44 bytes	technology&amp;ts=compact&a
320	www.bbc.com	application/json	2132 bytes	components?alternativeJsLoadi
340	odb.outbrain.com	text/x-json	22 kB	get?url=http%253A%252F%252
360	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=6
367	sa.bbc.co.uk	image/gif	43 bytes	s?name=news.blogs.trending.st
440	images.outbrain.com	image/jpeg	14 kB	177
454	odb.outbrain.com	text/x-json	20 kB	get?url=http%253A%252F%252
494	images.outbrain.com	image/jpeg	18 kB	177
562	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=1
585	images.outbrain.com	image/jpeg	9375 bytes	177
621	odb.outbrain.com	text/x-json	30 kB	get?url=http%253A%252F%252
631	images.outbrain.com	image/jpeg	23 kB	177
640	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=1
672	images.outbrain.com	image/jpeg	7718 bytes	90

A list of HTTP objects

Getting files from packet captures


airportSniffENFGOR-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Wireshark · Save Capture File As
Look in: /root
Computer
root
Open
Cancel
Help

```
No.  Time
  1 0.000000                         limited during cap…
  2 0.357877
  3 0.378808                         CK] Seq=1 Ack=2 Wi…
  4 0.592293
  5 0.612183                         CK] Seq=1 Ack=2 Wi…
  6 1.029793                         of a reassembled P…
  7 1.049964                         ACK] Seq=1 Ack=2 W…
  8 1.561052
  9 1.574332                         CK] Seq=1 Ack=2 Wi…

▸ Frame 1: 77 bytes o
▸ IEEE 802.3 Ethernet
▸ Logical-Link Contro
▸ 3Com XNS Encapsulat
▸ Data (32 bytes)
  [Packet size limite
```

Name	Size	Type	Date
scanning		Folder	10/2
Templates		Folder	6/23
Videos		Folder	6/23
vmware-tools-distrib		Folder	1/29
airportSniffdZH641.cap	38.5 MB	cap File	11/2
airportSniffENFGOR-dec.cap	4.4 MB	cap File	11/2
airportSniffENFGOR.cap	6.4 MB	cap File	11/2
airportSniffyG7m8J-dec.cap	1.3 MB	cap File	11/2
airportSniffyG7m8J.cap	3.0 MB	cap File	11/2
Lesson13a		Folder	11/2

File name:

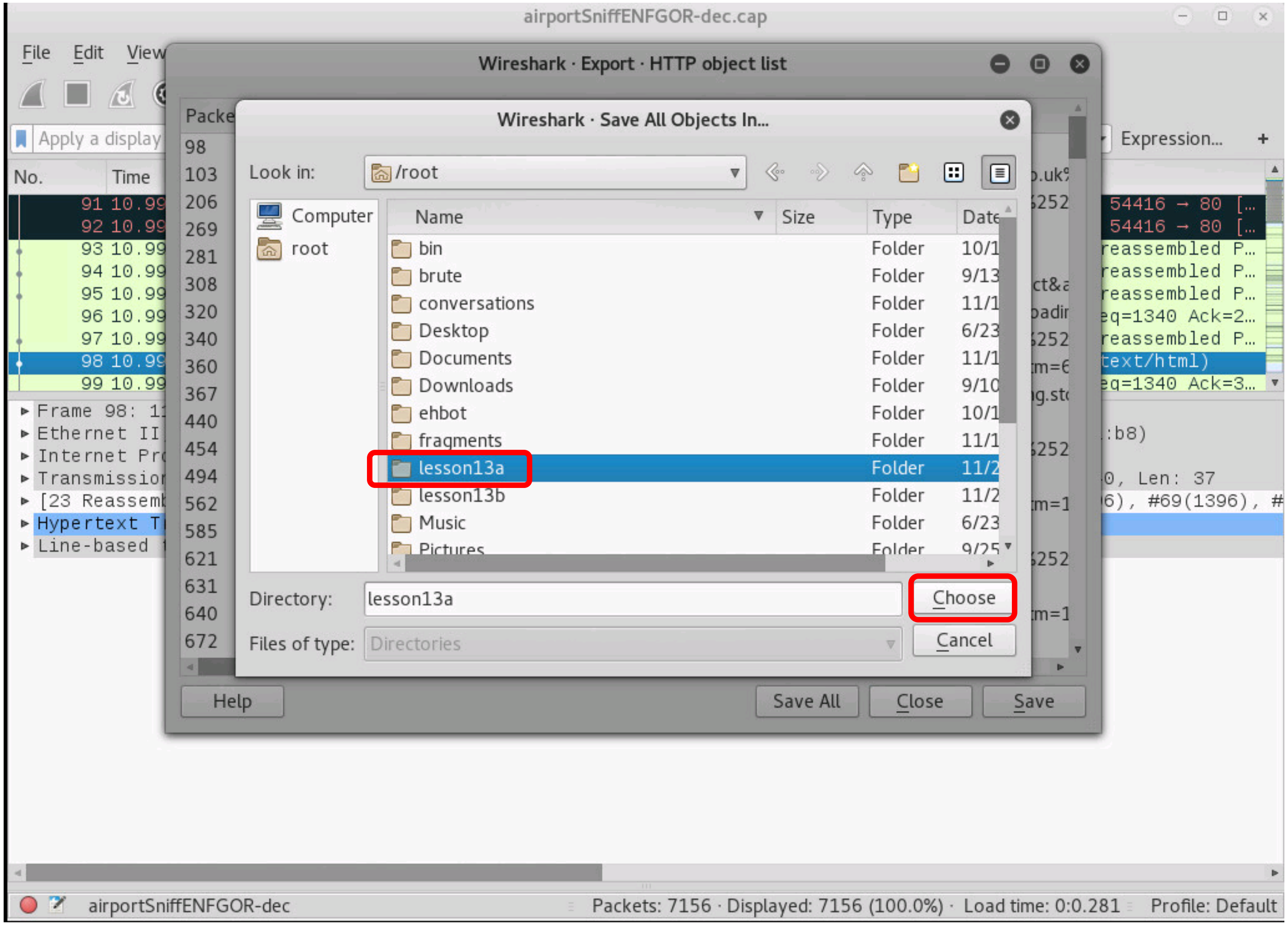
Save as: Wireshark/tcpdump/... - pcap (*.pcap *.pcap.gz *.cap *.cap.gz *.

☐ Compress with gzip

airportSniffENFGOR-dec   Packets: 7156 · Displayed: 7156 (100.0%) · Load time: 0:0.281   Profile: Default

There are a lot of objects so let's create a new directory to save them in.

Getting files from packet captures



Choose the new directory to save the objects in.

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap**

3) Run Wireshark on the decrypted airportSniffENFGOR-dec.cap file.

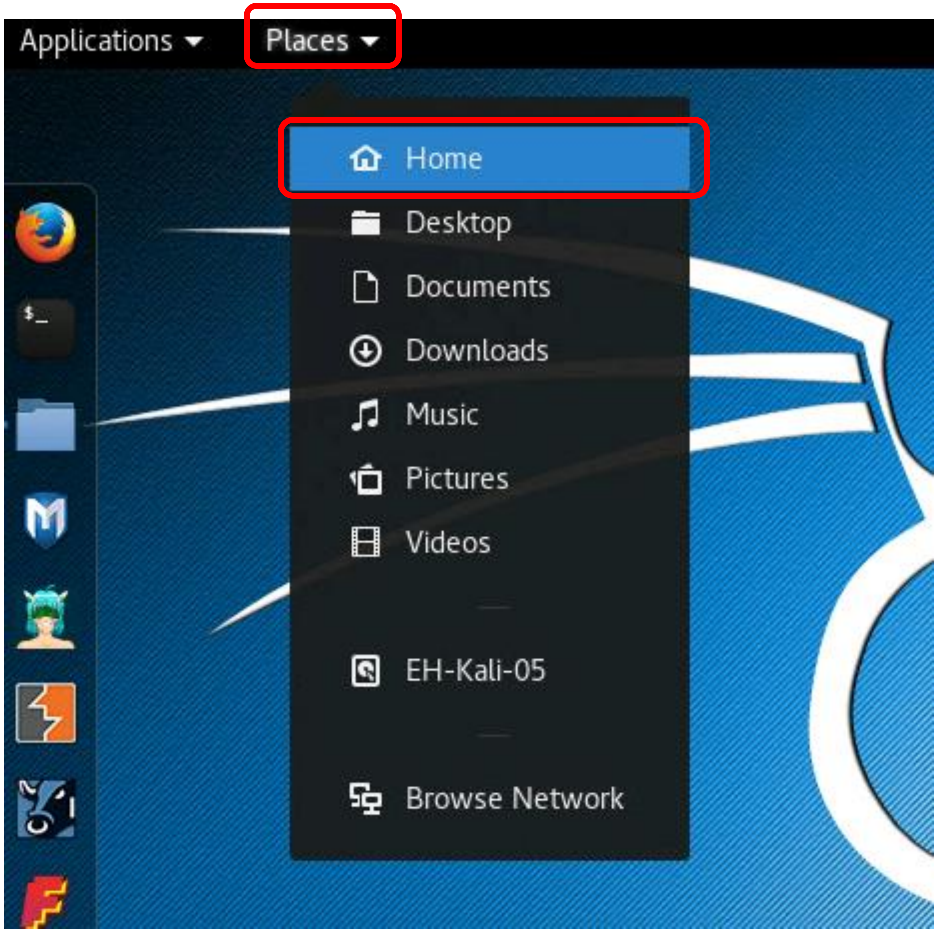
4) File > Export Objects > HTTP

5) Create a new lesson13a directory.

6) Save all the objects in the new directory.

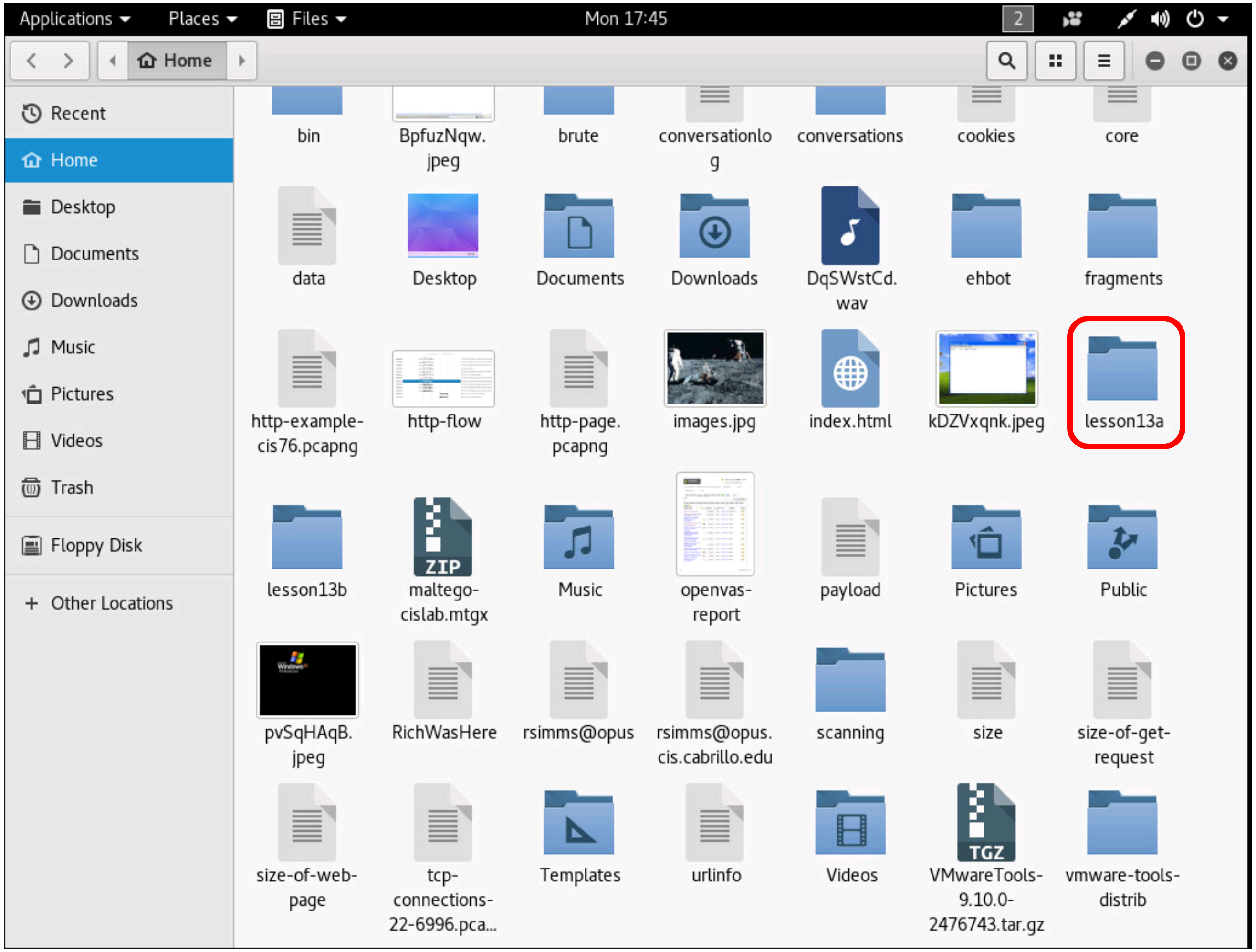
When finished note it in the chat window.

Getting files from packet captures



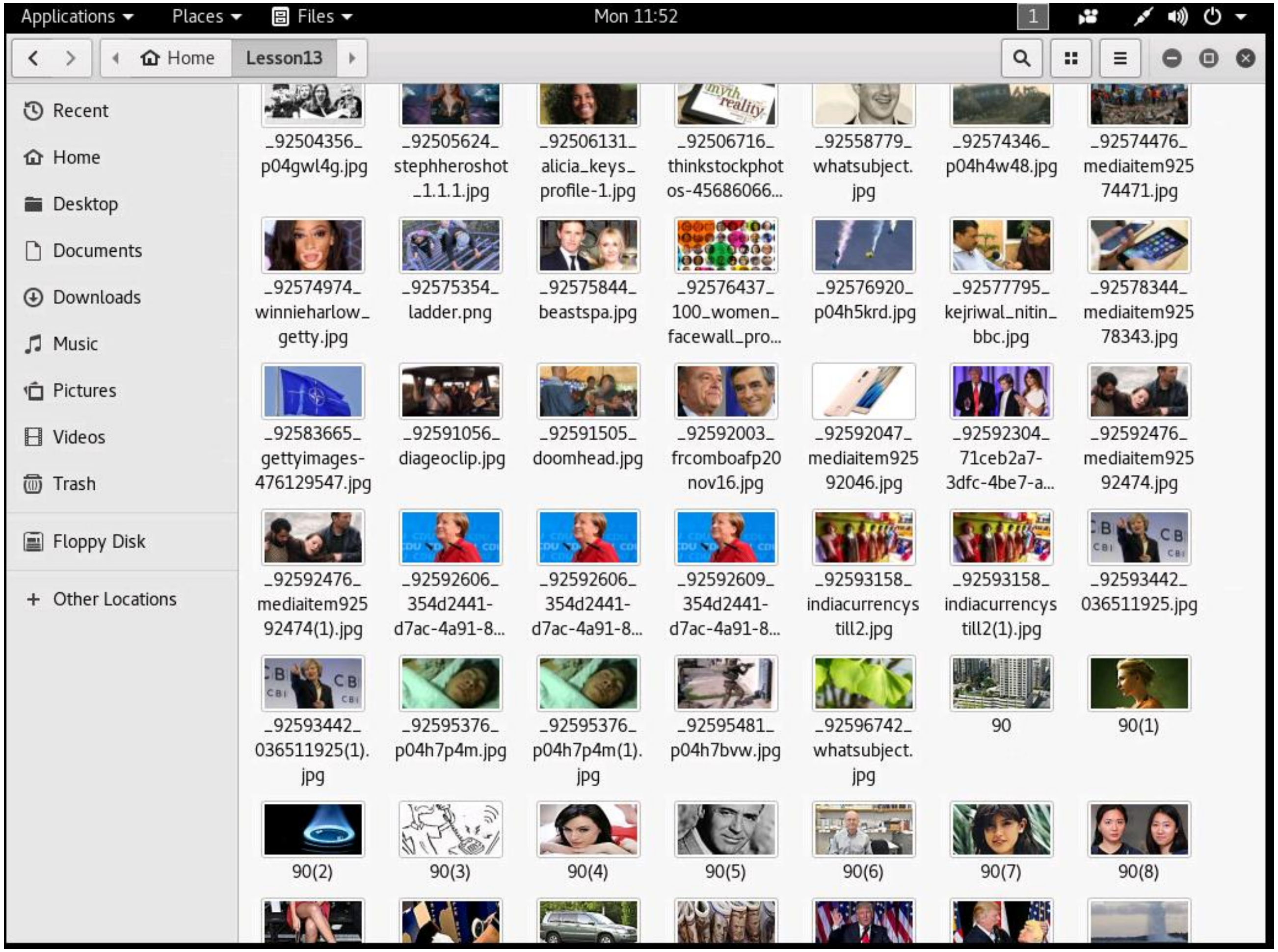
From the Kali desktop select Places > Home

Getting files from packet captures



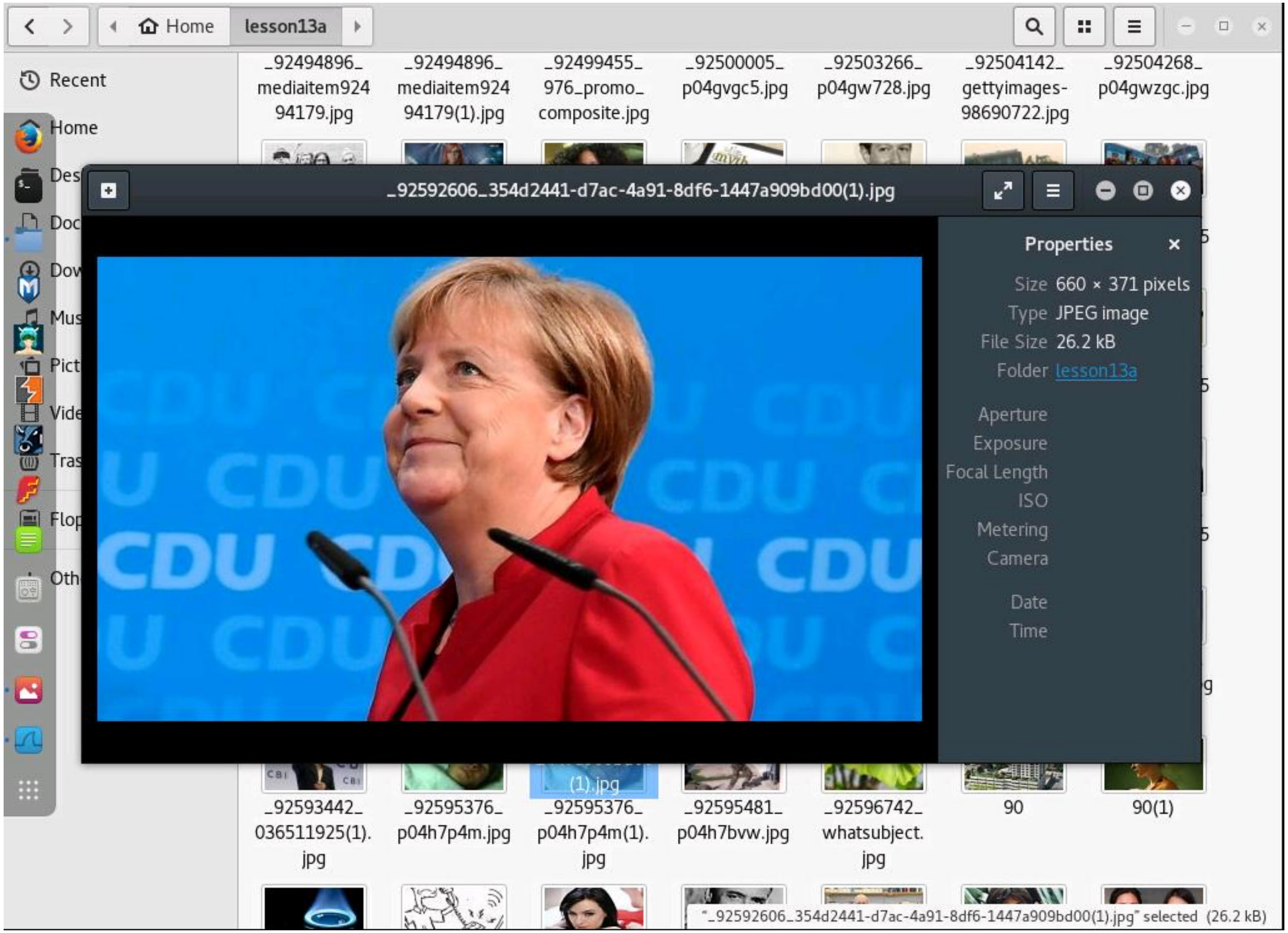
Open the new directory where the objects were saved

Getting files from packet captures


Applications
Places
Files
Mon 11:52
1
Home
Lesson13
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
+ Other Locations
_92504356_p04gwl4g.jpg
_92505624_stephheroshot_1.1.1.jpg
_92506131_alicia_keys_profile-1.jpg
_92506716_thinkstockphotos-45686066...
_92558779_whatsubject.jpg
_92574346_p04h4w48.jpg
_92574476_mediaitem92574471.jpg
_92574974_winnieharlow_getty.jpg
_92575354_ladder.png
_92575844_beastspa.jpg
_92576437_100_women_facewall_pro...
_92576920_p04h5krd.jpg
_92577795_kejriwal_nitin_bbc.jpg
_92578344_mediaitem92578343.jpg
_92583665_gettyimages-476129547.jpg
_92591056_diageoclip.jpg
_92591505_doomhead.jpg
_92592003_frcomboafp20nov16.jpg
_92592047_mediaitem92592046.jpg
_92592304_71ceb2a7-3dfc-4be7-a...
_92592476_mediaitem92592474.jpg
_92592476_mediaitem92592474(1).jpg
_92592606_354d2441-d7ac-4a91-8...
_92592606_354d2441-d7ac-4a91-8...
_92592609_354d2441-d7ac-4a91-8...
_92593158_indiacurrencystill2.jpg
_92593158_indiacurrencystill2(1).jpg
_92593442_036511925.jpg
_92593442_036511925(1).jpg
_92595376_p04h7p4m.jpg
_92595376_p04h7p4m(1).jpg
_92595481_p04h7bvw.jpg
_92596742_whatsubject.jpg
90
90(1)
90(2)
90(3)
90(4)
90(5)
90(6)
90(7)
90(8)

View the objects found in the decrypted packet capture

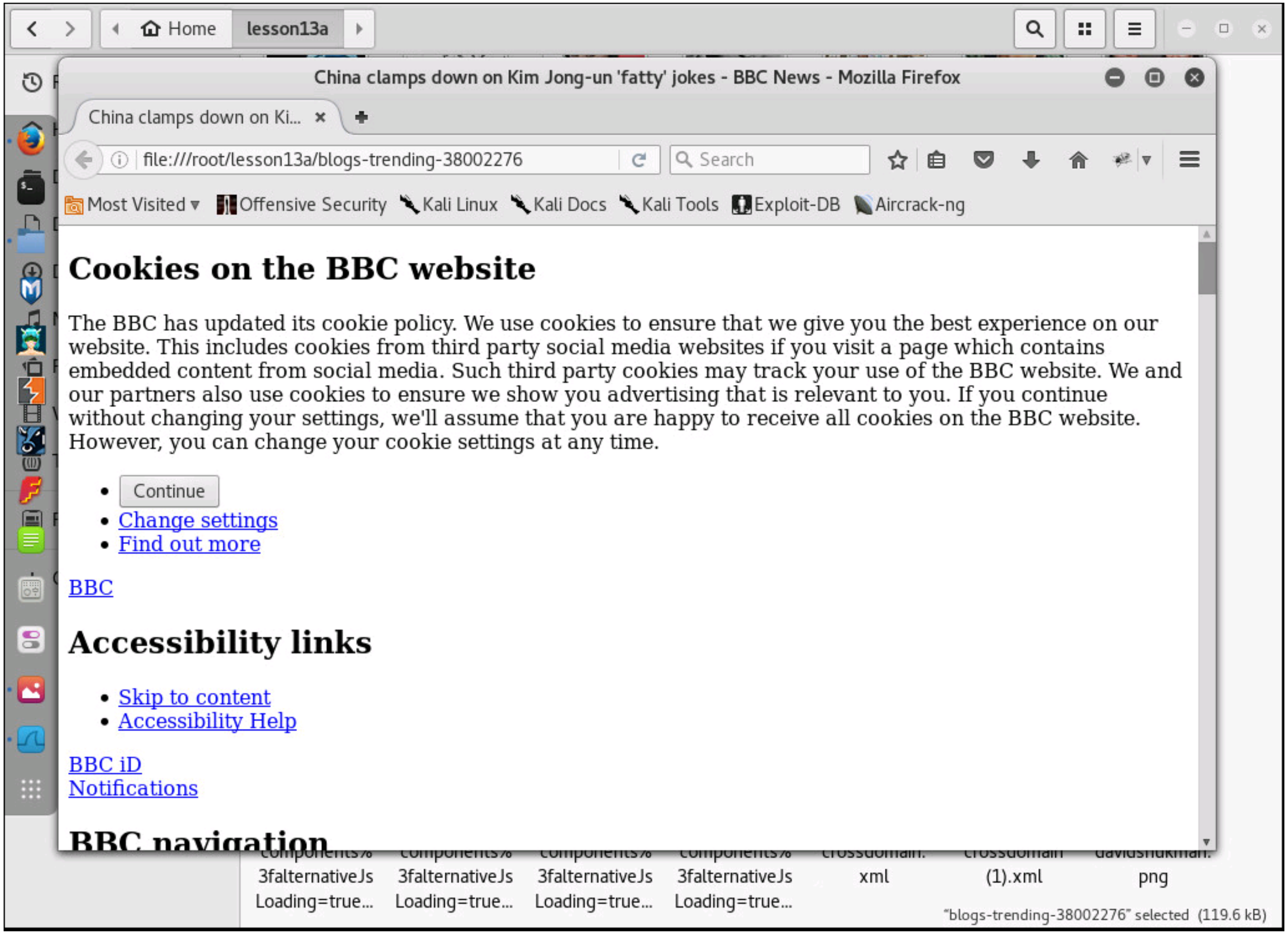
Getting files from packet captures



Home
lesson13a
Recent
_92494896_ mediaitem92494179.jpg
_92494896_ mediaitem92494179(1).jpg
_92499455_ 976_promo_ composite.jpg
_92500005_ p04gvgc5.jpg
_92503266_ p04gw728.jpg
_92504142_ gettyimages-98690722.jpg
_92504268_ p04gwzgc.jpg
_92592606_354d2441-d7ac-4a91-8df6-1447a909bd00(1).jpg
Properties
Size 660 × 371 pixels
Type JPEG image
File Size 26.2 kB
Folder lesson13a
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time
_92593442_ 036511925(1).jpg
_92595376_ p04h7p4m.jpg
_92595376_ p04h7p4m(1).jpg
_92595481_ p04h7bvw.jpg
_92596742_ whatsubject.jpg
90
90(1)
"_92592606_354d2441-d7ac-4a91-8df6-1447a909bd00(1).jpg" selected (26.2 kB)

A JPEG file used in a BBC article

Getting files from packet captures


Home
lesson13a
China clamps down on Kim Jong-un 'fatty' jokes - BBC News - Mozilla Firefox
China clamps down on Ki...
file:///root/lesson13a/blogs-trending-38002276
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

Cookies on the BBC website

The BBC has updated its cookie policy. We use cookies to ensure that we give you the best experience on our website. This includes cookies from third party social media websites if you visit a page which contains embedded content from social media. Such third party cookies may track your use of the BBC website. We and our partners also use cookies to ensure we show you advertising that is relevant to you. If you continue without changing your settings, we'll assume that you are happy to receive all cookies on the BBC website. However, you can change your cookie settings at any time.

- Continue
- Change settings
- Find out more

BBC

Accessibility links

- Skip to content
- Accessibility Help

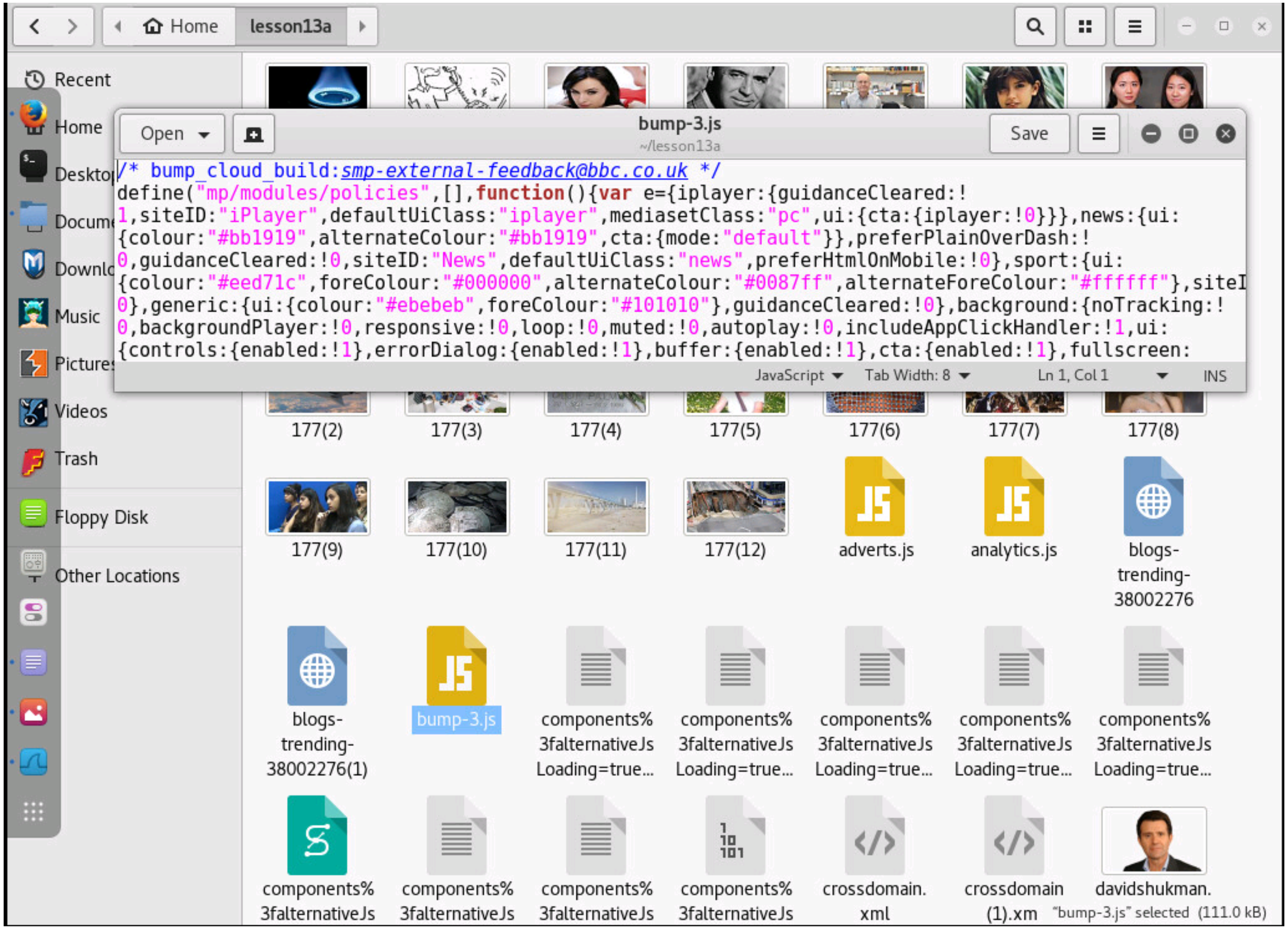
BBC iD
Notifications

BBC navigation

components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
crossdomain. xml
crossdomain (1).xml
davidshukman. png
"blogs-trending-38002276" selected (119.6 kB)

Webpage on BBC website

Getting files from packet captures

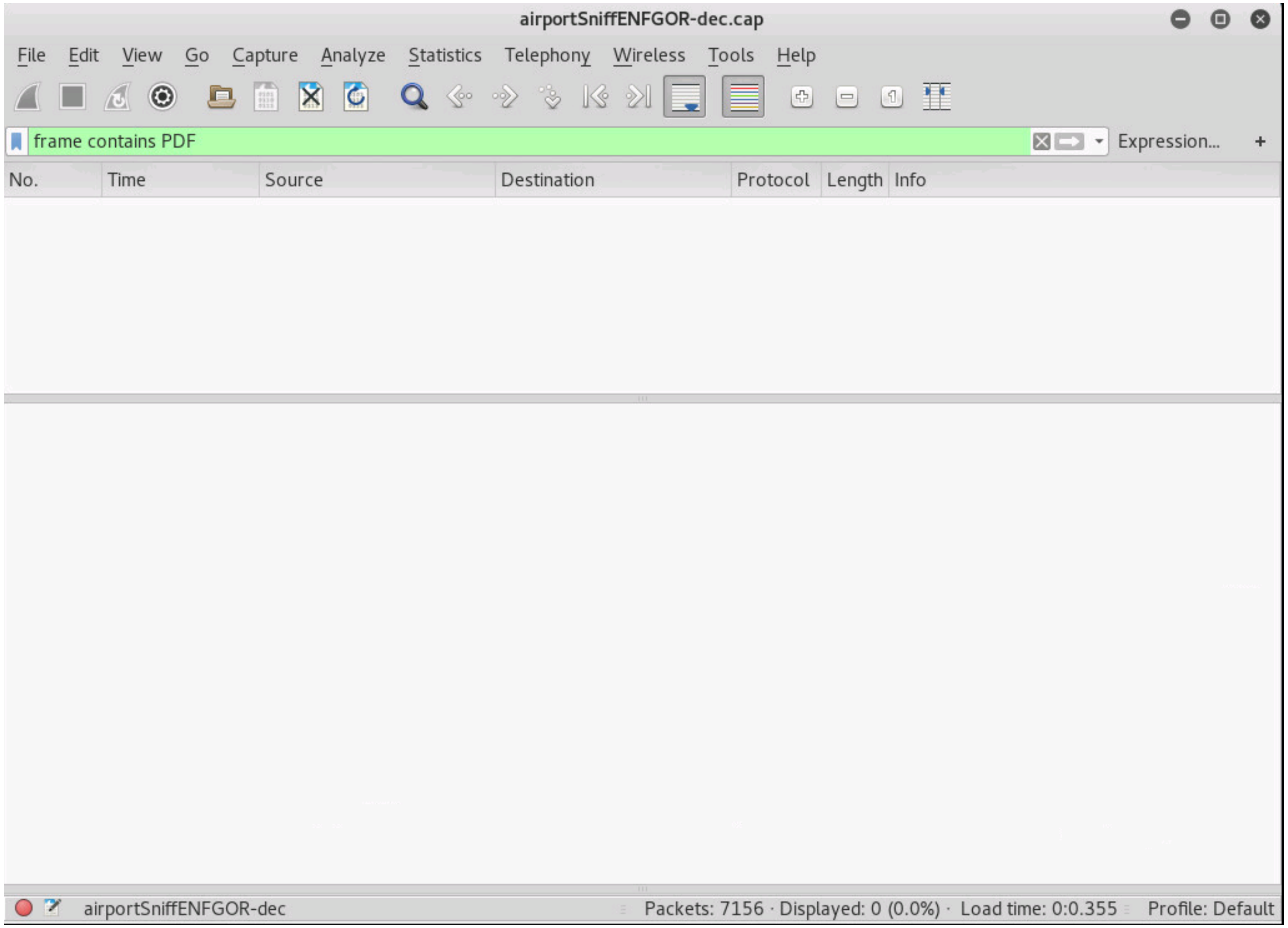


```
/* bump_cloud_build:smp-external-feedback@bbc.co.uk */
define("mp/modules/policies",[],function(){var e={iplayer:{guidanceCleared:!
1,siteID:"iPlayer",defaultUiClass:"iplayer",mediasetClass:"pc",ui:{cta:{iplayer:!0}}},news:{ui:
{colour:"#bb1919",alternateColour:"#bb1919",cta:{mode:"default"}},preferPlainOverDash:!
0,guidanceCleared:!0,siteID:"News",defaultUiClass:"news",preferHtmlOnMobile:!0},sport:{ui:
{colour:"#eed71c",foreColour:"#000000",alternateColour:"#0087ff",alternateForeColour:"#ffffff"},siteI
0},generic:{ui:{colour:"#ebebeb",foreColour:"#101010"},guidanceCleared:!0},background:{noTracking:!
0,backgroundPlayer:!0,responsive:!0,loop:!0,muted:!0,autoplay:!0,includeAppClickHandler:!1,ui:
{controls:{enabled:!1},errorDialog:{enabled:!1},buffer:{enabled:!1},cta:{enabled:!1},fullscreen:
```

Home
lesson13a
Recent
Home
Deskto
Docum
Downl
Music
Picture
Videos
Trash
Floppy Disk
Other Locations
Open
bump-3.js
~/lesson13a
Save
JavaScript
Tab Width: 8
Ln 1, Col 1
INS
177(2)
177(3)
177(4)
177(5)
177(6)
177(7)
177(8)
177(9)
177(10)
177(11)
177(12)
adverts.js
analytics.js
blogs-trending-38002276
blogs-trending-38002276(1)
bump-3.js
components%3falternativeJs Loading=true...
components%3falternativeJs Loading=true...
components%3falternativeJs Loading=true...
components%3falternativeJs Loading=true...
components%3falternativeJs Loading=true...
components%3falternativeJs
components%3falternativeJs
components%3falternativeJs
components%3falternativeJs
crossdomain.xml
crossdomain (1).xm
davidshukman.
"bump-3.js" selected (111.0 kB)

A JavaScript file on ten website

Filtering for PDF documents


airportSniffENFGOR-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

frame contains PDF

No. | Time | Source | Destination | Protocol | Length | Info

airportSniffENFGOR-dec

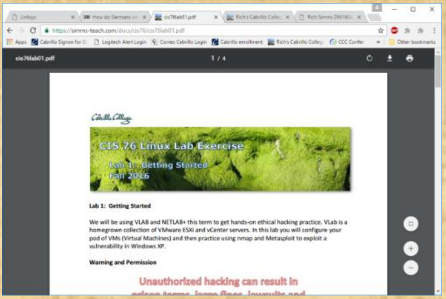
Packets: 7156 · Displayed: 0 (0.0%) · Load time: 0:0.355

Profile: Default

But the PDF from my website was not found!

Activity

https://simms-teach.com/docs/cis76/cis76lab01.pdf



Cabrillo College

CIS 76 Linux Lab Exercise

Lab 1: Getting Started
Fall 2016

Lab 1: Getting Started

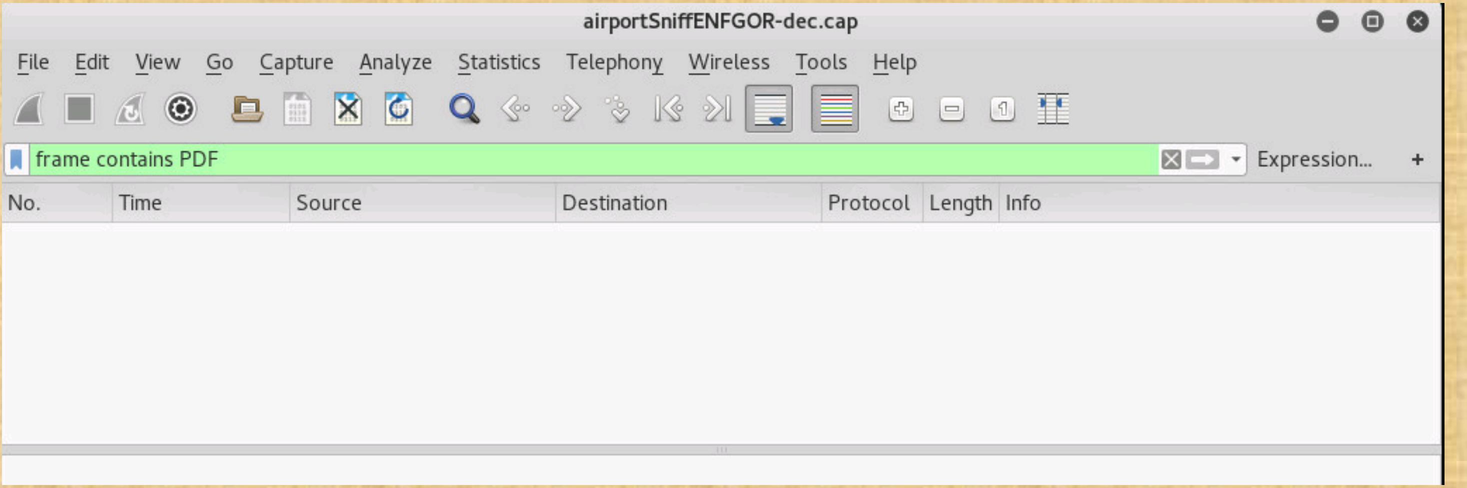
We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pod of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in

Why are there no PDF frames in the capture?

Write your answer in the chat window.


airportSniffENFGOR-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

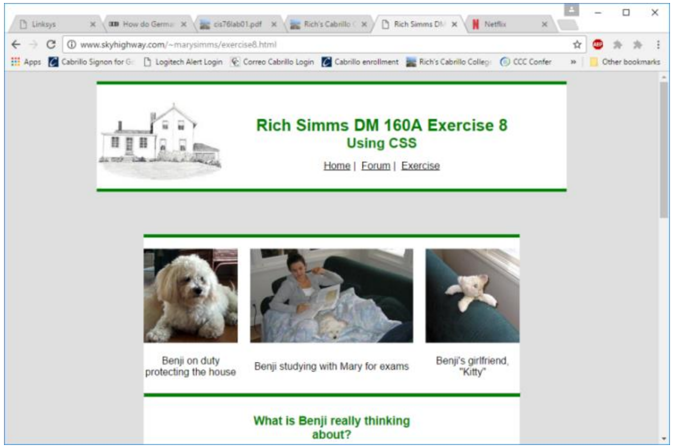
frame contains PDF

No. | Time | Source | Destination | Protocol | Length | Info

Capture

yG7m8J

airportSniffyG7m8J.cap



www.skyhighway.com/~marysimms/exercise8.html

Rich Simms DM 160A Exercise 8
Using CSS

Home | Forum | Exercise

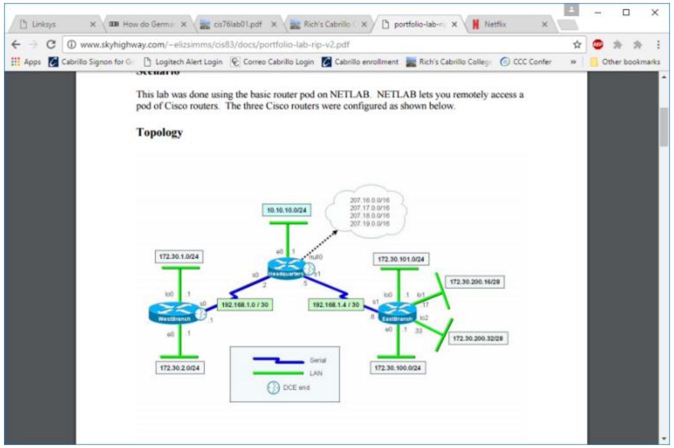
Benji on duty protecting the house

Benji studying with Mary for exams

Benji's girlfriend, "Kitty"

What is Benji really thinking about?

http://www.skyhighway.com/~marysimms/exercise8.html



www.skyhighway.com/~elizsimms/cis83/docs/portfolio-lab-rip-v2.pdf

This lab was done using the basic router pod on NETLAB. NETLAB lets you remotely access a pod of Cisco routers. The three Cisco routers were configured as shown below.

Topology

http://www.skyhighway.com/~elizsimms/cis83/docs
/portfolio-lab-VLAN.pdf

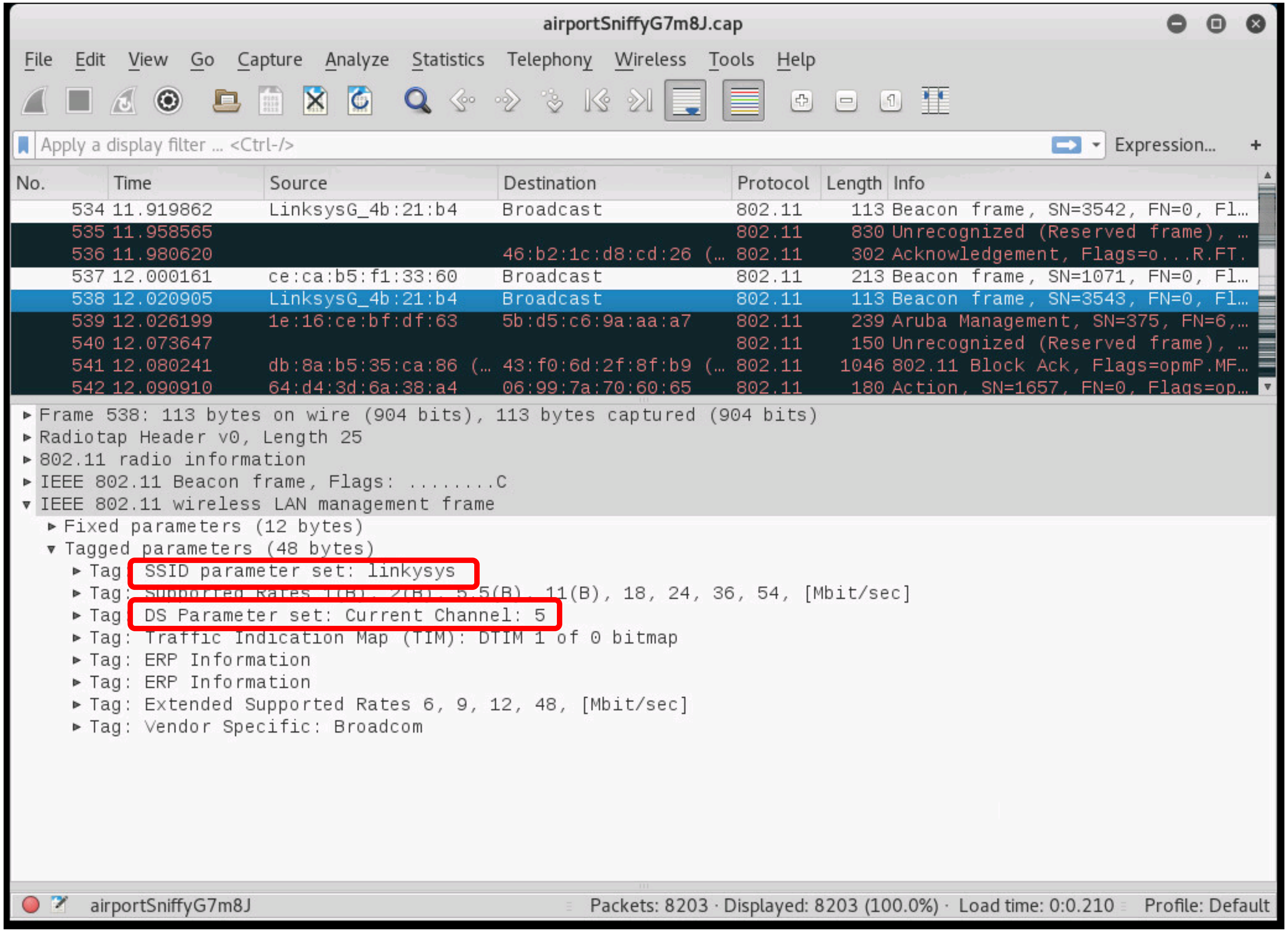
ls -l airportSniffyG7m8J.cap

```
root@eh-kali-05:~# ls -l airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 3095355 Nov 21 12:31 airportSniffyG7m8J.cap
root@eh-kali-05:~#
```

file airportSniffyG7m8J.cap

```
root@eh-kali-05:~# file airportSniffyG7m8J.cap
airportSniffyG7m8J.cap: tcpdump capture file (little-endian) - version 2.4 (802.11 with
radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

Listing the packet capture file



airportSniffyG7m8J.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

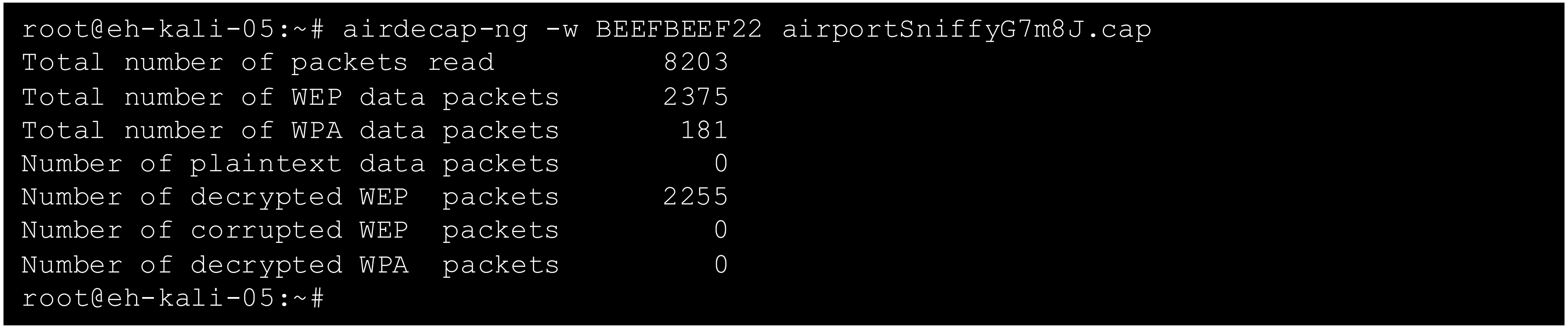
```
No.    Time       Source                Destination           Protocol Length Info
   534 11.919862  LinksysG_4b:21:b4     Broadcast             802.11    113 Beacon frame, SN=3542, FN=0, Fl…
   535 11.958565                                              802.11    830 Unrecognized (Reserved frame), …
   536 11.980620                        46:b2:1c:d8:cd:26 (…  802.11    302 Acknowledgement, Flags=o...R.FT.
   537 12.000161  ce:ca:b5:f1:33:60     Broadcast             802.11    213 Beacon frame, SN=1071, FN=0, Fl…
   538 12.020905  LinksysG_4b:21:b4     Broadcast             802.11    113 Beacon frame, SN=3543, FN=0, Fl…
   539 12.026199  1e:16:ce:bf:df:63     5b:d5:c6:9a:aa:a7     802.11    239 Aruba Management, SN=375, FN=6,…
   540 12.073647                                              802.11    150 Unrecognized (Reserved frame), …
   541 12.080241  db:8a:b5:35:ca:86 (…  43:f0:6d:2f:8f:b9 (…  802.11   1046 802.11 Block Ack, Flags=opmP.MF…
   542 12.090910  64:d4:3d:6a:38:a4     06:99:7a:70:60:65     802.11    180 Action, SN=1657, FN=0, Flags=op…
```

```
▸ Frame 538: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (48 bytes)
    ▸ Tag: SSID parameter set: linkysys
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 5
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: Vendor Specific: Broadcom
```

airportSniffyG7m8J
Packets: 8203 · Displayed: 8203 (100.0%) · Load time: 0:0.210
Profile: Default

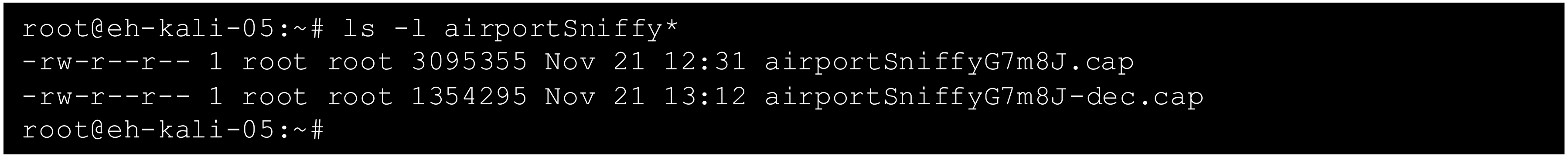
Beacon frame in encrypted packet capture file

airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap



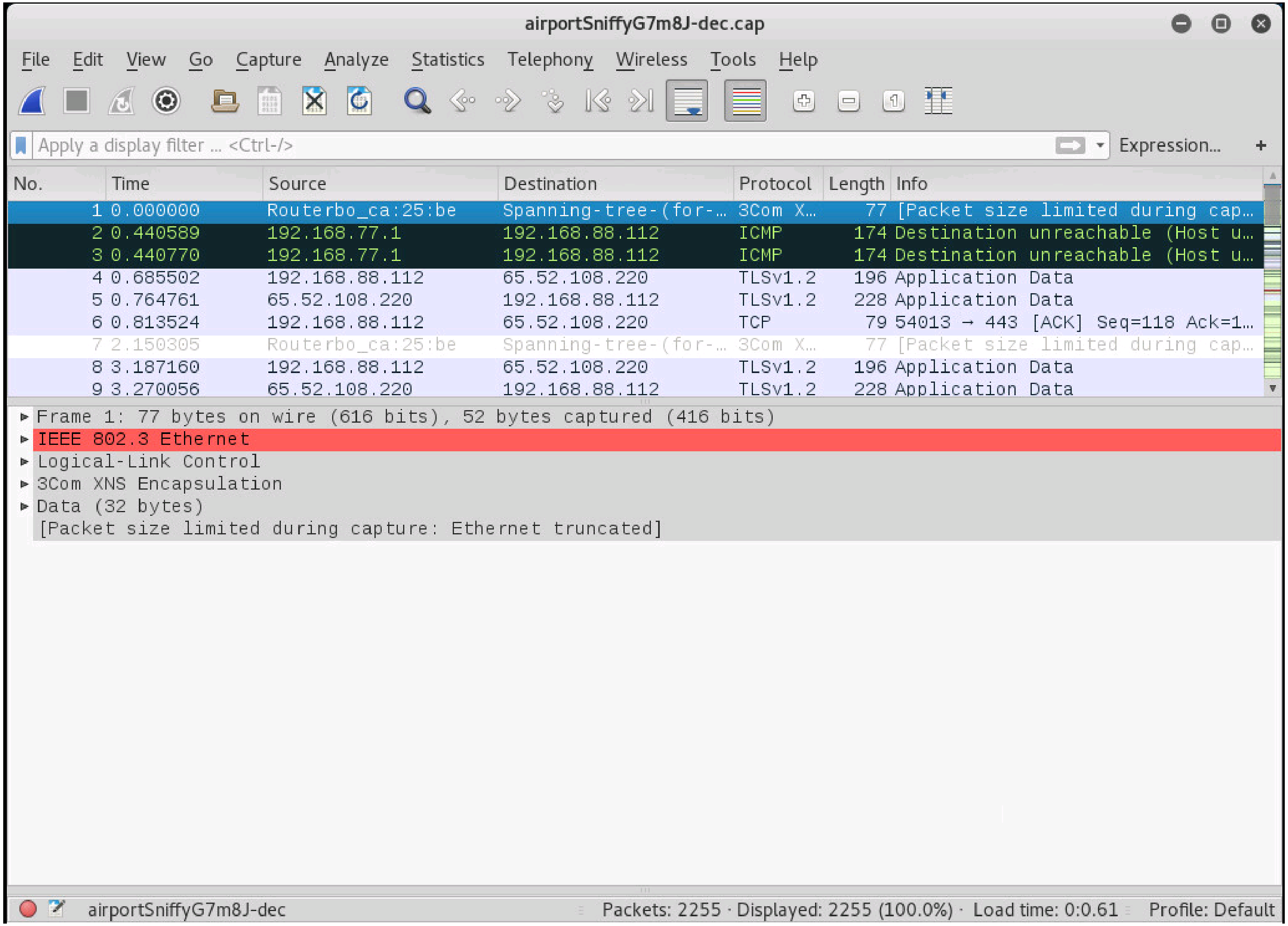
```
root@eh-kali-05:~# airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap
Total number of packets read          8203
Total number of WEP data packets      2375
Total number of WPA data packets       181
Number of plaintext data packets         0
Number of decrypted WEP  packets      2255
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@eh-kali-05:~#
```

ls -l airportSniffy*



```
root@eh-kali-05:~# ls -l airportSniffy*
-rw-r--r-- 1 root root 3095355 Nov 21 12:31 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 1354295 Nov 21 13:12 airportSniffyG7m8J-dec.cap
root@eh-kali-05:~#
```

Decrypting the packet capture file

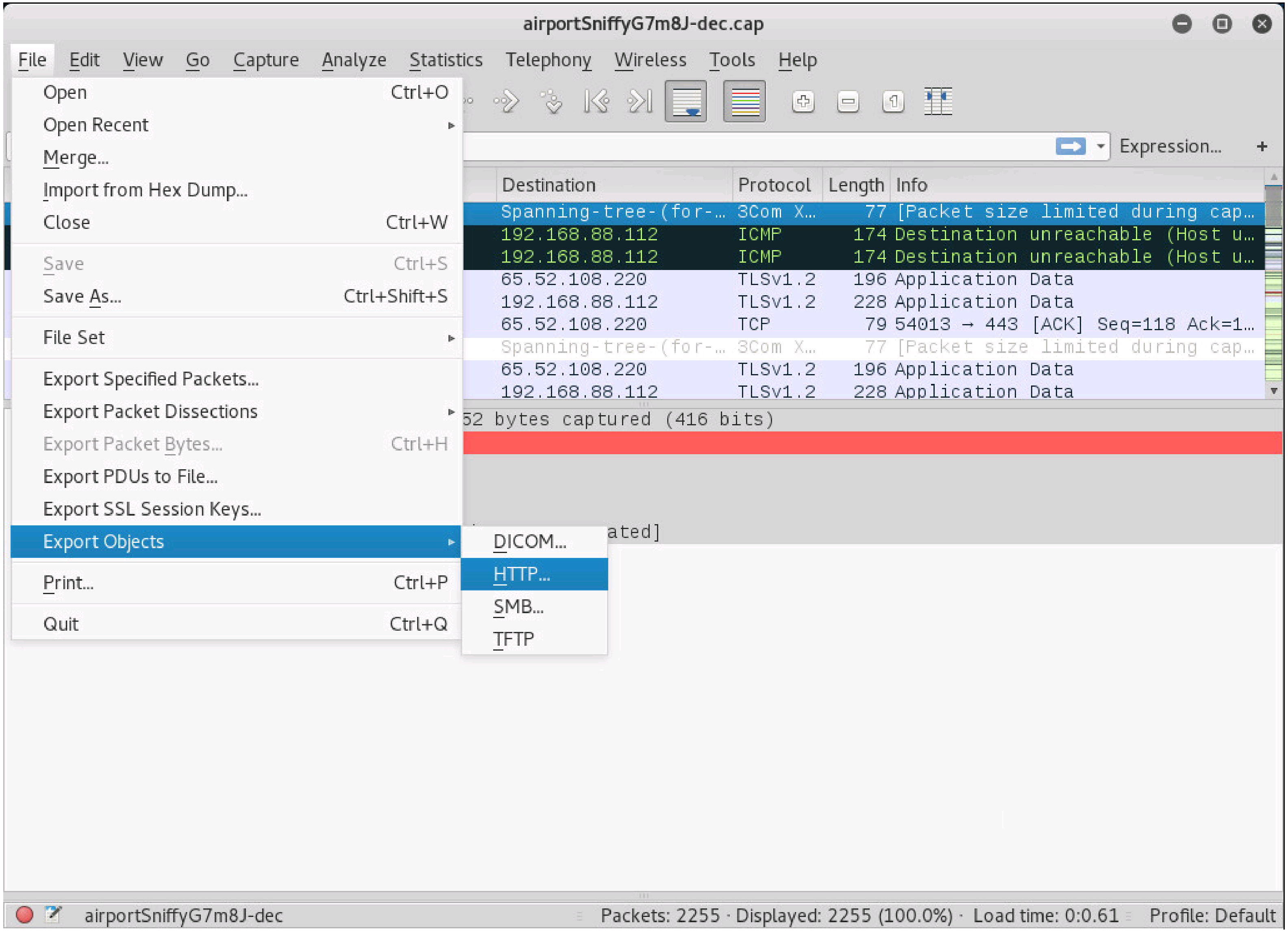

airportSniffyG7m8J-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time       Source              Destination            Protocol  Length Info
    1 0.000000   Routerbo_ca:25:be   Spanning-tree-(for-…   3Com X…       77 [Packet size limited during cap…
    2 0.440589   192.168.77.1        192.168.88.112         ICMP         174 Destination unreachable (Host u…
    3 0.440770   192.168.77.1        192.168.88.112         ICMP         174 Destination unreachable (Host u…
    4 0.685502   192.168.88.112      65.52.108.220          TLSv1.2      196 Application Data
    5 0.764761   65.52.108.220       192.168.88.112         TLSv1.2      228 Application Data
    6 0.813524   192.168.88.112      65.52.108.220          TCP           79 54013 → 443 [ACK] Seq=118 Ack=1…
    7 2.150305   Routerbo_ca:25:be   Spanning-tree-(for-…   3Com X…       77 [Packet size limited during cap…
    8 3.187160   192.168.88.112      65.52.108.220          TLSv1.2      196 Application Data
    9 3.270056   65.52.108.220       192.168.88.112         TLSv1.2      228 Application Data
```

```
▸ Frame 1: 77 bytes on wire (616 bits), 52 bytes captured (416 bits)
▸ IEEE 802.3 Ethernet
▸ Logical-Link Control
▸ 3Com XNS Encapsulation
▸ Data (32 bytes)
  [Packet size limited during capture: Ethernet truncated]
```

```
airportSniffyG7m8J-dec     Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61     Profile: Default
```

Decrypted packet capture showing normal traffic

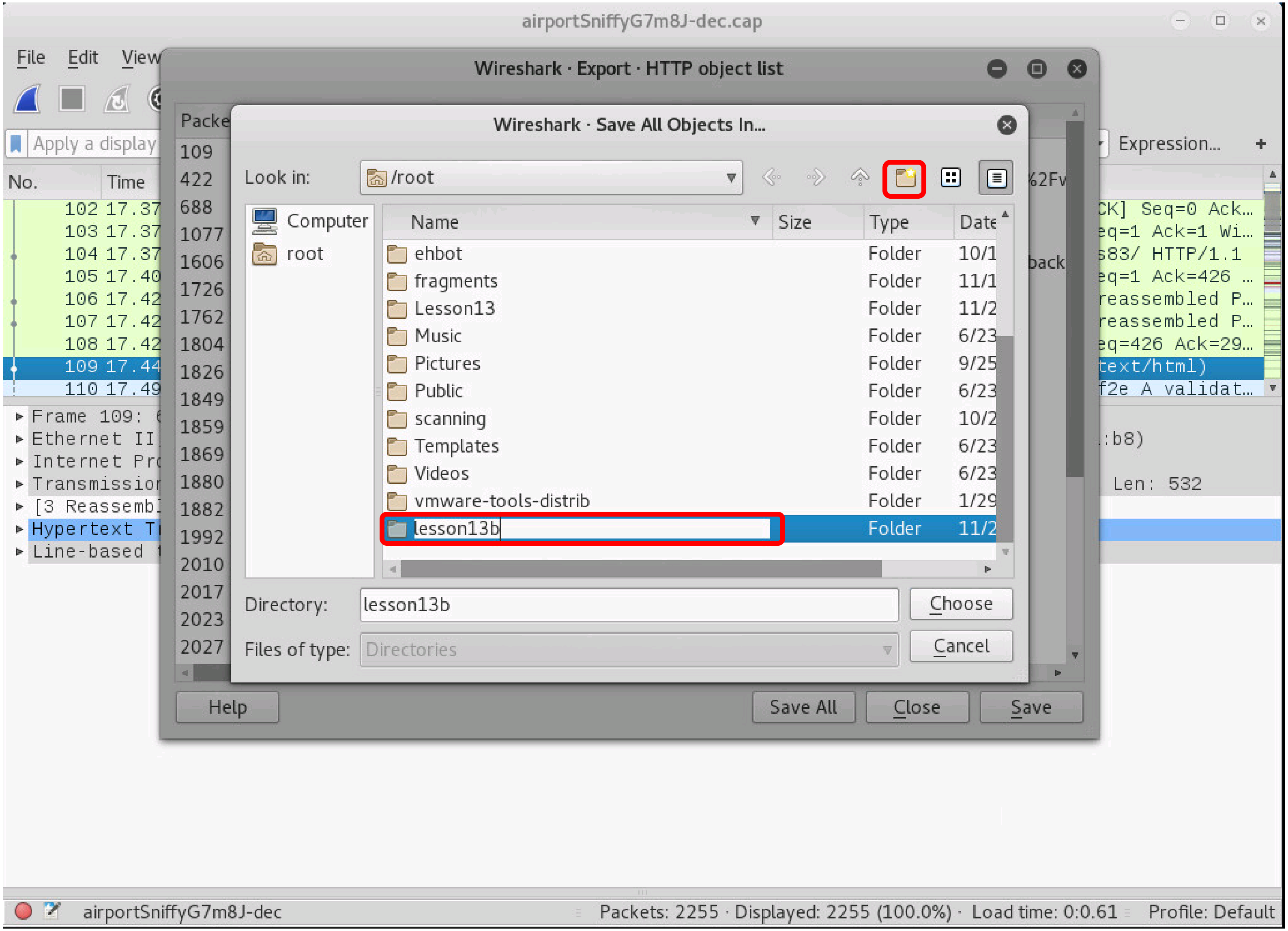


Destination	Protocol	Length	Info
Spanning-tree-(for-…	3Com X…	77	[Packet size limited during cap…
192.168.88.112	ICMP	174	Destination unreachable (Host u…
192.168.88.112	ICMP	174	Destination unreachable (Host u…
65.52.108.220	TLSv1.2	196	Application Data
192.168.88.112	TLSv1.2	228	Application Data
65.52.108.220	TCP	79	54013 → 443 [ACK] Seq=118 Ack=1…
Spanning-tree-(for-…	3Com X…	77	[Packet size limited during cap…
65.52.108.220	TLSv1.2	196	Application Data
192.168.88.112	TLSv1.2	228	Application Data

```
52 bytes captured (416 bits)
ated]
```

airportSniffyG7m8J-dec   Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61   Profile: Default

Extracting objects from the capture



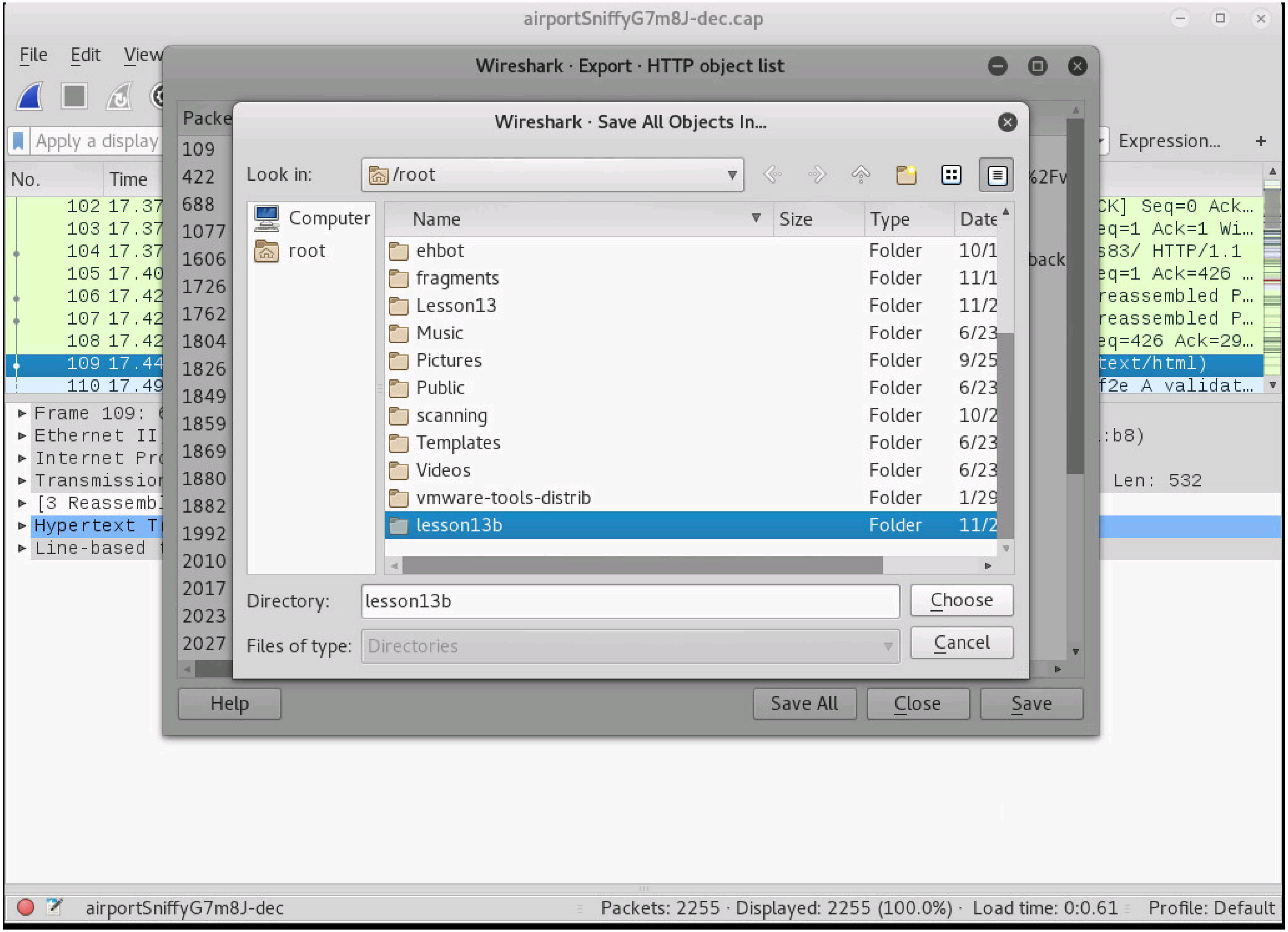
Name	Size	Type	Date
ehbot		Folder	10/1
fragments		Folder	11/1
Lesson13		Folder	11/2
Music		Folder	6/23
Pictures		Folder	9/25
Public		Folder	6/23
scanning		Folder	10/2
Templates		Folder	6/23
Videos		Folder	6/23
vmware-tools-distrib		Folder	1/29
lesson13b		Folder	11/2

Directory: lesson13b

Files of type: Directories

airportSniffyG7m8J-dec · Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61 · Profile: Default

Make a new directory



airportSniffyG7m8J-dec.cap

Wireshark · Export · HTTP object list

Wireshark · Save All Objects In...

Look in: /root

Name	Size	Type	Date
ehbot		Folder	10/1
fragments		Folder	11/1
Lesson13		Folder	11/2
Music		Folder	6/23
Pictures		Folder	9/25
Public		Folder	6/23
scanning		Folder	10/2
Templates		Folder	6/23
Videos		Folder	6/23
vmware-tools-distrib		Folder	1/29
lesson13b		Folder	11/2

Directory: lesson13b

Files of type: Directories

Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61 · Profile: Default

Save all to the new directory

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap**

3) Run Wireshark on the decrypted airportSniffyG7m8J-dec.cap file.

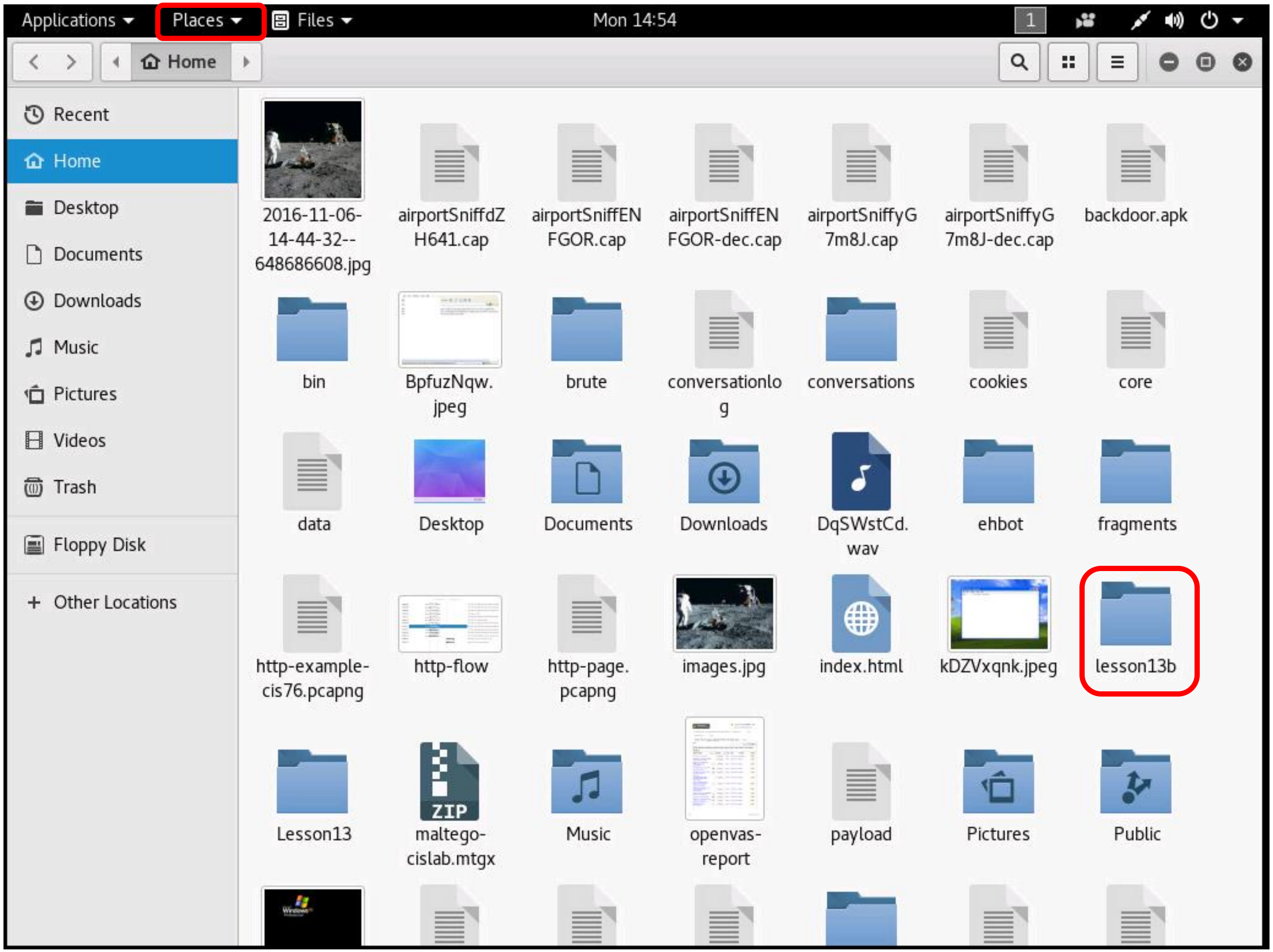
4) File > Export Objects > HTTP

5) Create a new lesson13b directory.

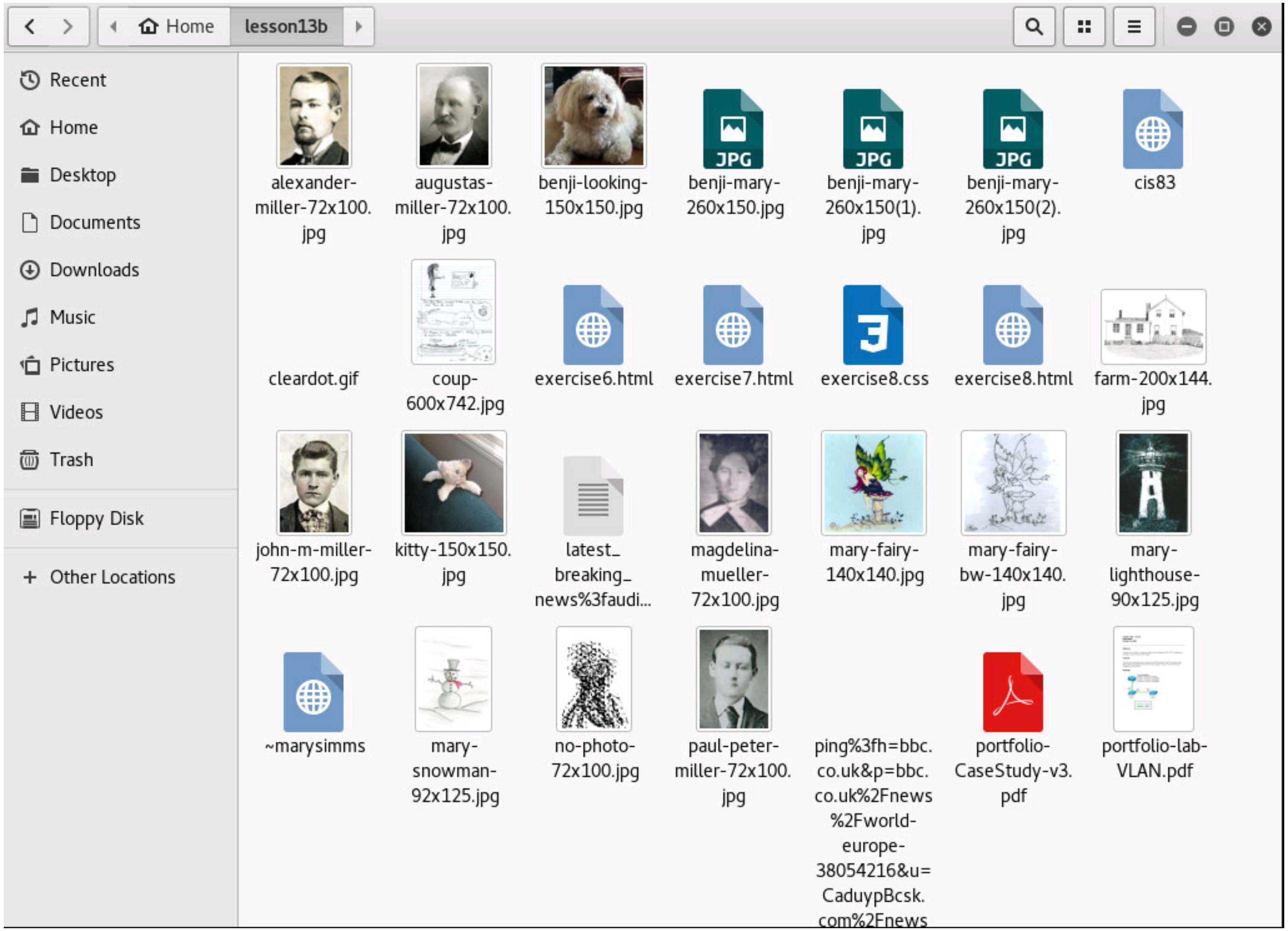
6) Save all the objects in the new directory.

When finished note it in the chat window.

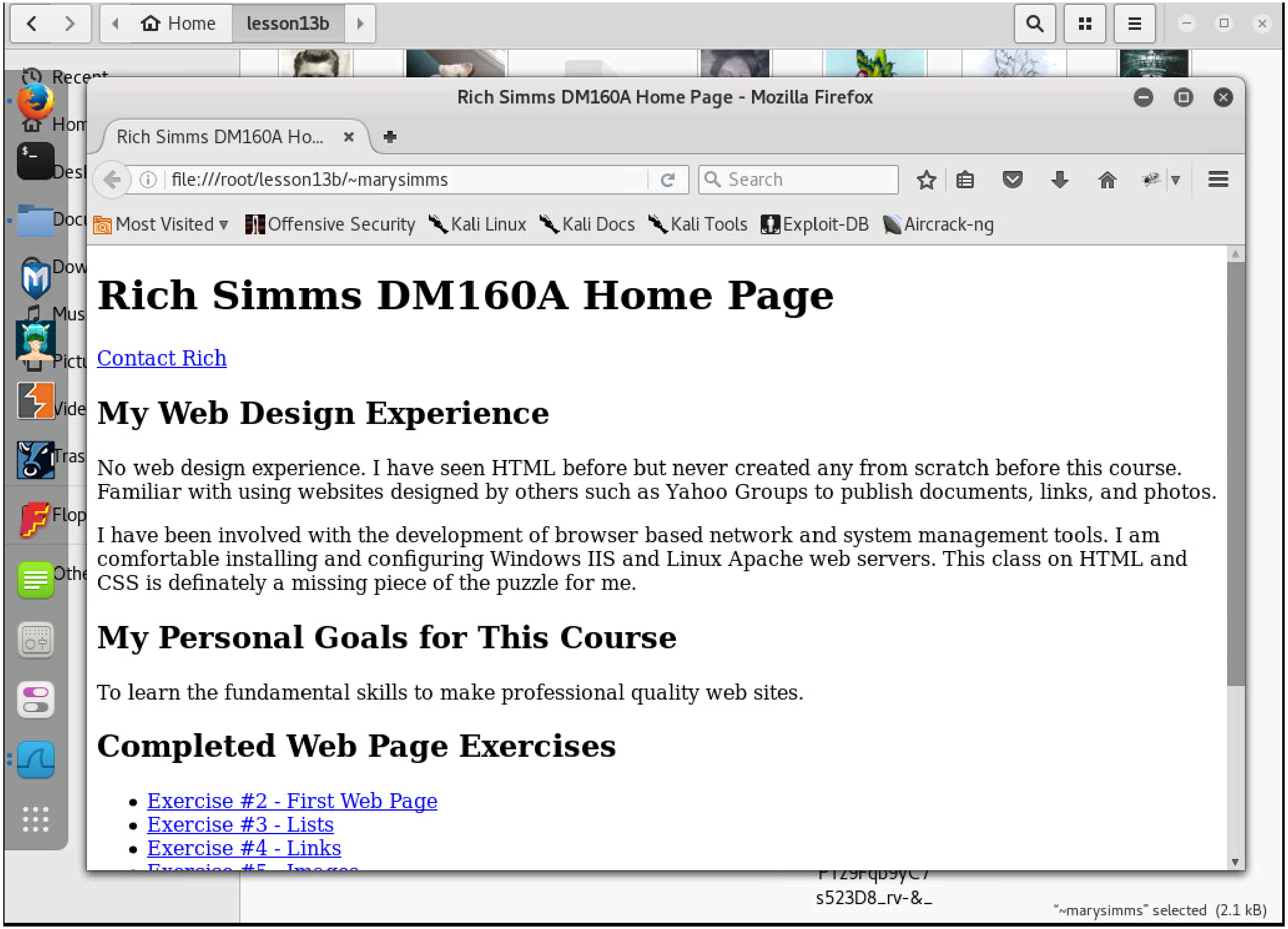
CIS 76 - Lesson 13



Places > home, then open the new folder



alexander-miller-72x100.jpg
augustas-miller-72x100.jpg
benji-looking-150x150.jpg
benji-mary-260x150.jpg
benji-mary-260x150(1).jpg
benji-mary-260x150(2).jpg
cis83
cleardot.gif
coup-600x742.jpg
exercise6.html
exercise7.html
exercise8.css
exercise8.html
farm-200x144.jpg
john-m-miller-72x100.jpg
kitty-150x150.jpg
latest_breaking_news%3faudi...
magdelina-mueller-72x100.jpg
mary-fairy-140x140.jpg
mary-fairy-bw-140x140.jpg
mary-lighthouse-90x125.jpg
~marysimms
mary-snowman-92x125.jpg
no-photo-72x100.jpg
paul-peter-miller-72x100.jpg
ping%3fh=bbc.co.uk&p=bbc.co.uk%2Fnews%2Fworld-europe-38054216&u=CaduypBcsk.com%2Fnews
portfolio-CaseStudy-v3.pdf
portfolio-lab-VLAN.pdf



Rich Simms DM160A Home Page

Contact Rich

My Web Design Experience

No web design experience. I have seen HTML before but never created any from scratch before this course. Familiar with using websites designed by others such as Yahoo Groups to publish documents, links, and photos.

I have been involved with the development of browser based network and system management tools. I am comfortable installing and configuring Windows IIS and Linux Apache web servers. This class on HTML and CSS is definately a missing piece of the puzzle for me.

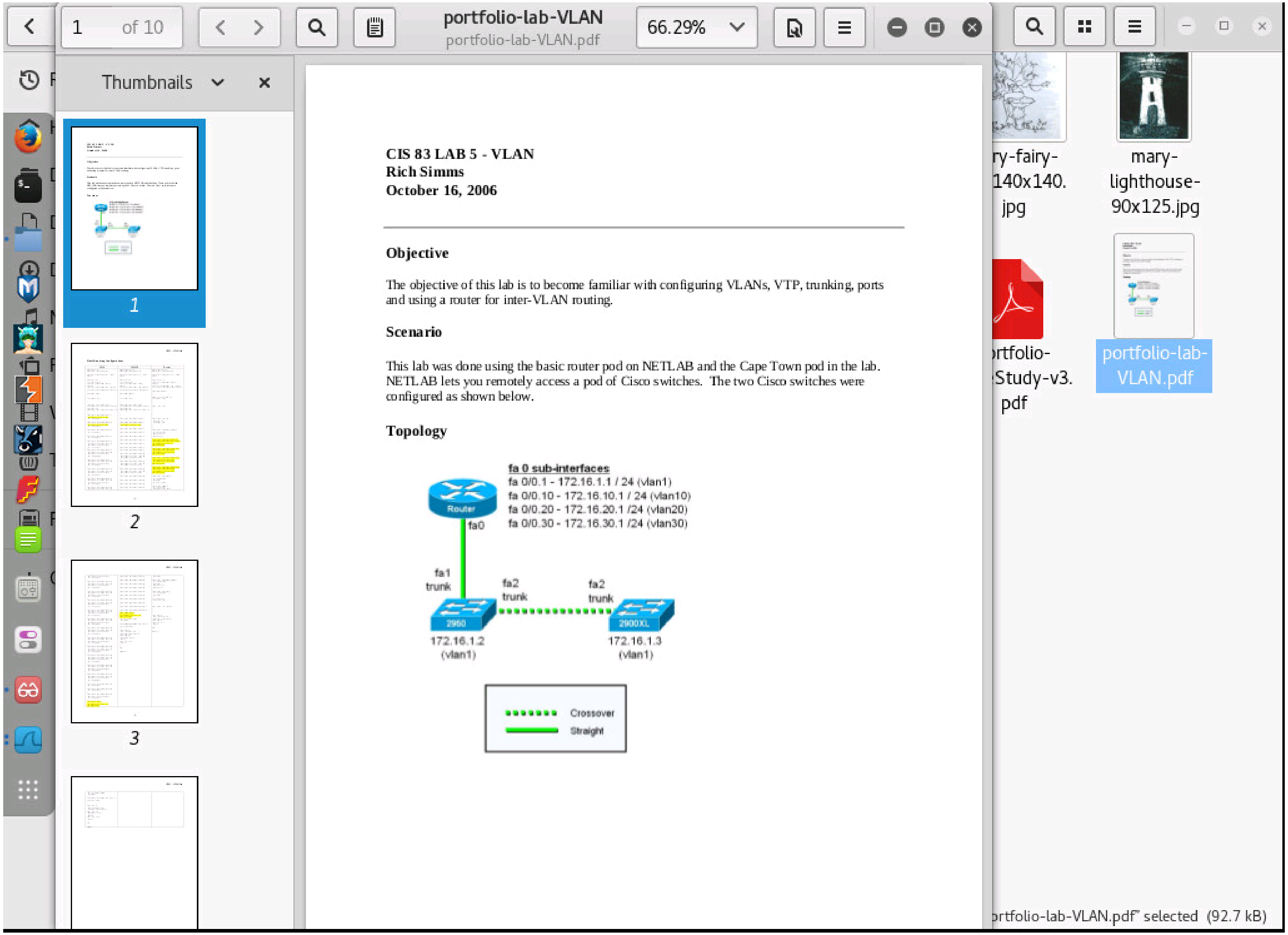
My Personal Goals for This Course

To learn the fundamental skills to make professional quality web sites.

Completed Web Page Exercises

- Exercise #2 - First Web Page
- Exercise #3 - Lists
- Exercise #4 - Links
- Exercise #5 - Images

web pages



CIS 83 LAB 5 - VLAN
Rich Simms
October 16, 2006

Objective

The objective of this lab is to become familiar with configuring VLANs, VTP, trunking, ports and using a router for inter-VLAN routing.

Scenario

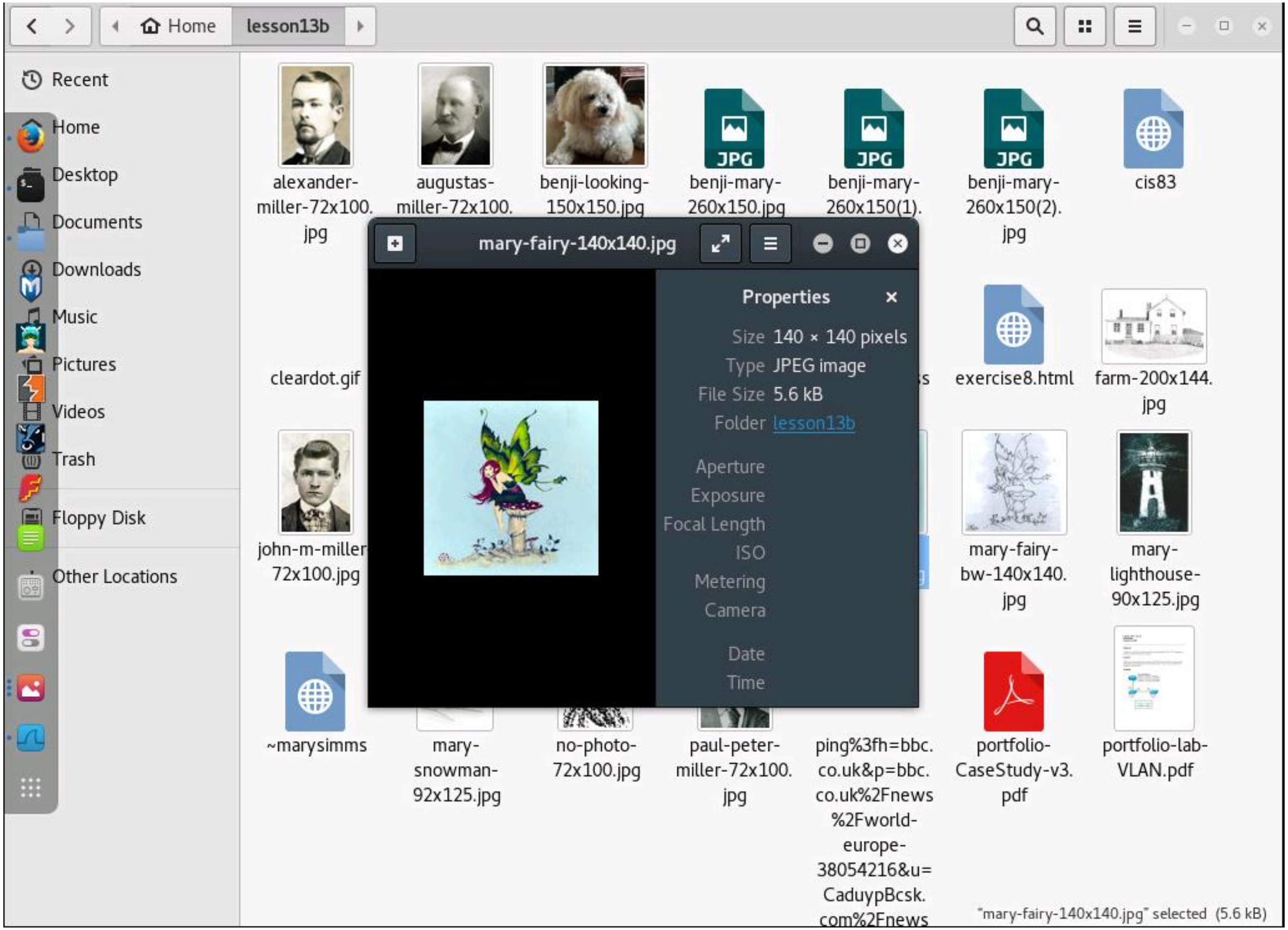
This lab was done using the basic router pod on NETLAB and the Cape Town pod in the lab. NETLAB lets you remotely access a pod of Cisco switches. The two Cisco switches were configured as shown below.

Topology

fa 0 sub-interfaces
fa 0/0.1 - 172.16.1.1 / 24 (vlan1)
fa 0/0.10 - 172.16.10.1 / 24 (vlan10)
fa 0/0.20 - 172.16.20.1 /24 (vlan20)
fa 0/0.30 - 172.16.30.1 /24 (vlan30)

Yes we have PDF files now too!

CIS 76 - Lesson 13



Size 140 × 140 pixels
Type JPEG image
File Size 5.6 kB
Folder lesson13b

Aperture
Exposure
Focal Length
ISO
Metering
Camera

Date
Time

JPEG files

Activity

As root, on your EH-Kali-XX VM:

1) Find the extracted coup-600x742.jpg file

2) Of the two options, what do you think Benji decided to do?

Write your answer in the chat window.

Wireless WPA/WPA2 Hack

Wi-Fi Protected Access (WPA)

WPA

- Developed in 2003 to replace WEP.
- Still uses WEP's insecure RC4 stream cipher
- Uses Temporal Key Integrity Protocol (TKIP) to provide extra security.
- More secure than WEP.

WPA2

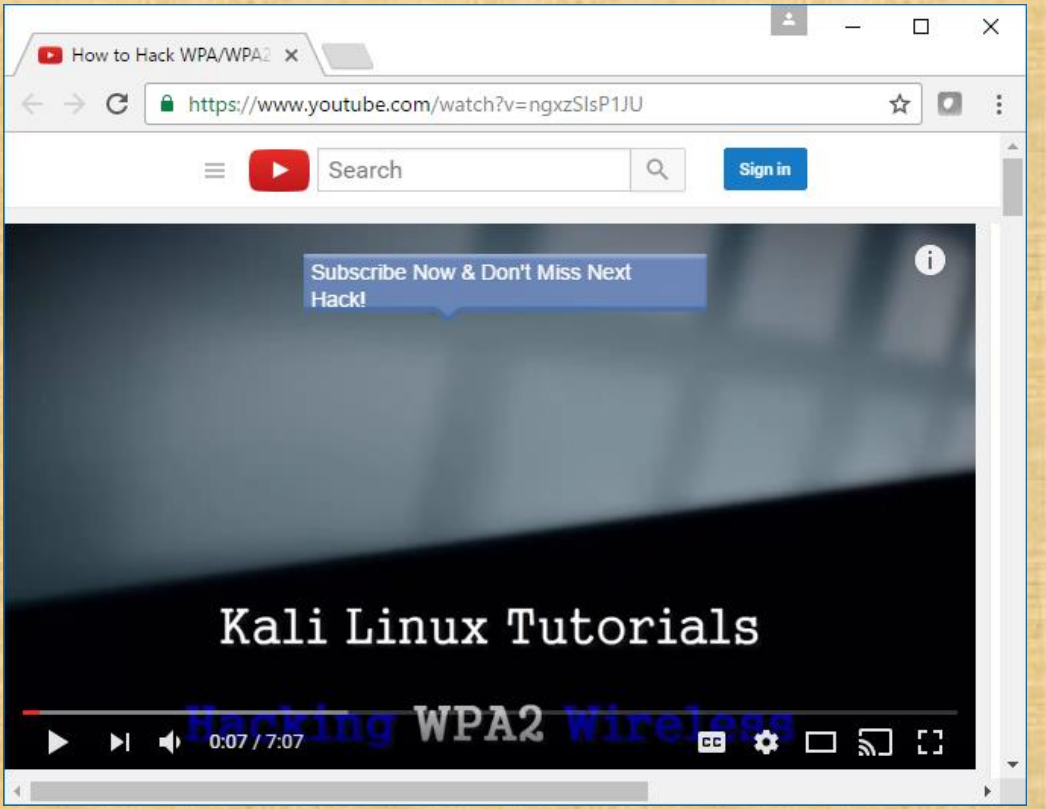
- Developed in 2004 to replace WEP and WPA.
- Uses AES instead of RC4.
- Replaces TKIP with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- More secure than WPA.

As of March 2006, all devices using the Wi-Fi trademark must be WPA2 certified

http://www.diffen.com/difference/WPA_vs_WPA2

How to Hack WPA/WPA2 Wi-Fi With Kali Linux Aircrack-ng

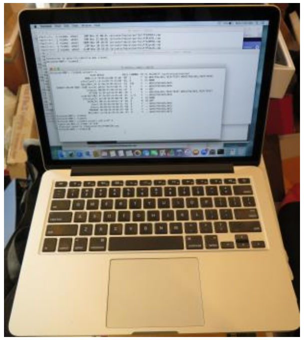
Ink That! Offensive Security



https://www.youtube.com/watch?v=ngxzSIsP1JU

Linksys WAP54G Access Point

BSSID
= Basic Service Set Identifier
= AP Mac Address
= 00:06:25:4b:21:b4

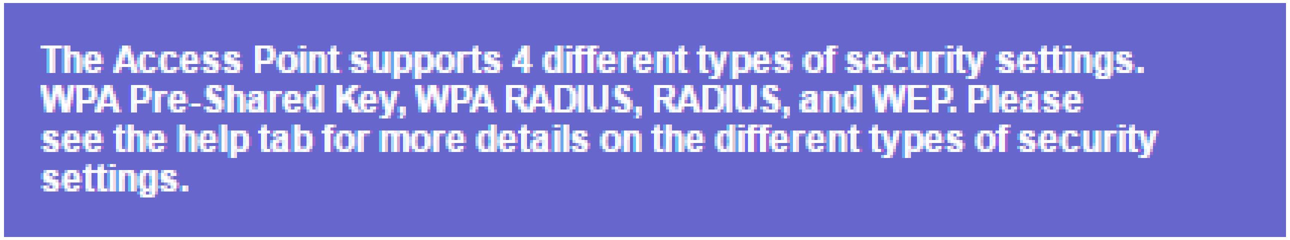


STA
= Station
= MacBook Pro

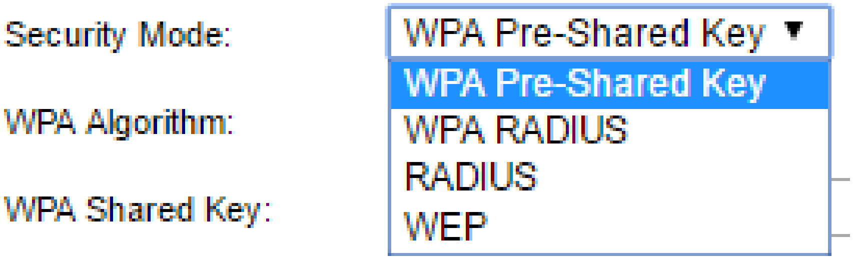
STA
= Station
= Win 10 PC

SSID
= Service Set Identifier
= Name of the network
= linkysys

Linksys WAP54G



The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.



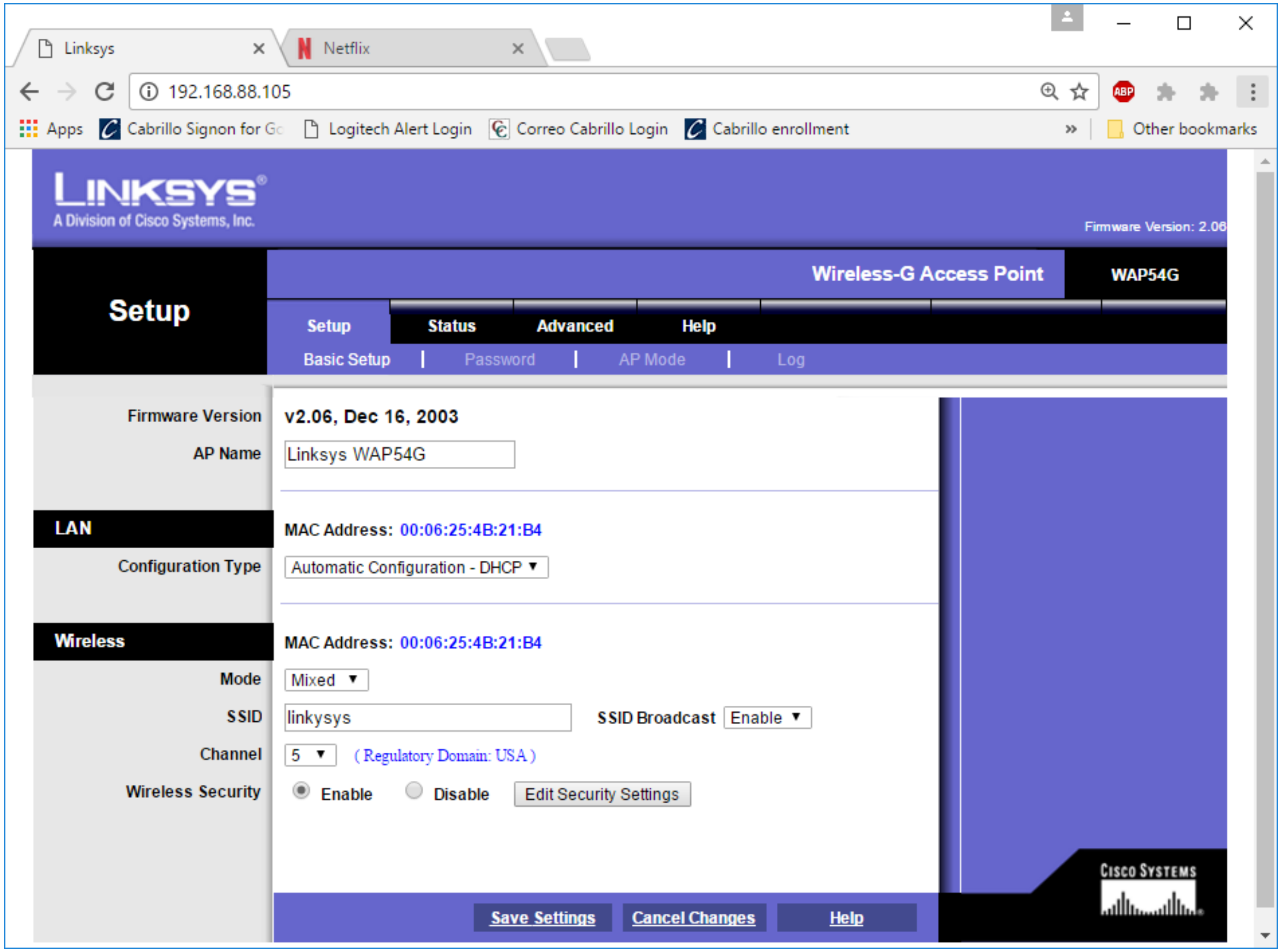
Security Mode: WPA Pre-Shared Key

WPA Algorithm:

WPA Shared Key:

For this example we will use WPA (WiFi Protected Access)

Linksys WAP54G



Firmware Version: v2.06, Dec 16, 2003

AP Name: Linksys WAP54G

LAN

MAC Address: 00:06:25:4B:21:B4

Configuration Type: Automatic Configuration - DHCP

Wireless

MAC Address: 00:06:25:4B:21:B4

Mode: Mixed

SSID: linkysys

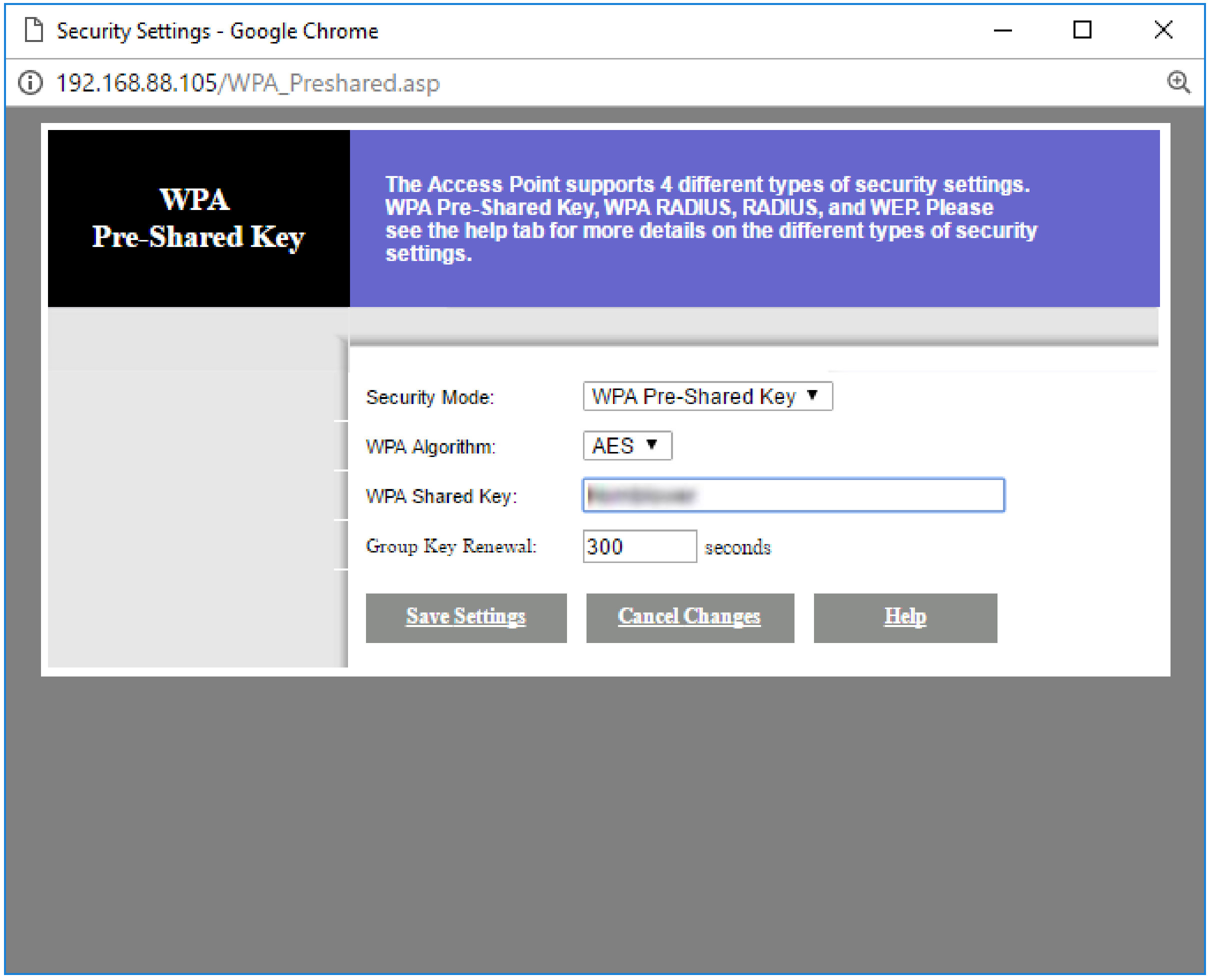
SSID Broadcast: Enable

Channel: 5 (Regulatory Domain: USA)

Wireless Security: ● Enable ○ Disable Edit Security Settings

Using Mixed Mode (B and G), Channel 5, and Wireless Security (WEP)

Linksys WAP54G



Security Settings - Google Chrome
192.168.88.105/WPA_Preshared.asp

WPA Pre-Shared Key

The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.

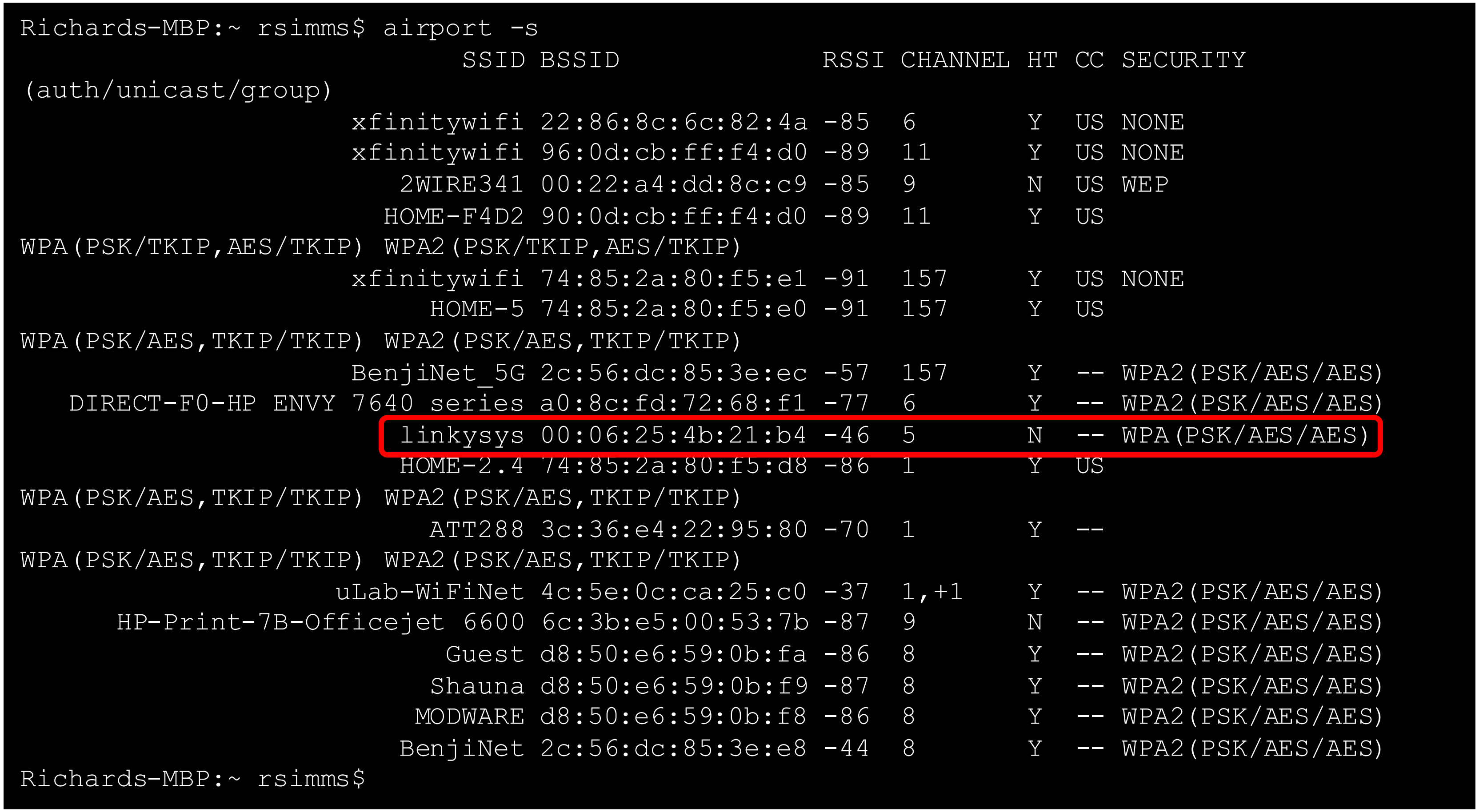
Security Mode:	WPA Pre-Shared Key ▼
WPA Algorithm:	AES ▼
WPA Shared Key:	[redacted]
Group Key Renewal:	300 seconds

Save Settings
Cancel Changes
Help

Select a WPA shared key

Sniffing using MacBook Pro

airport -s



```
Richards-MBP:~ rsimms$ airport -s
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY
(auth/unicast/group)
                     xfinitywifi 22:86:8c:6c:82:4a -85  6       Y  US NONE
                     xfinitywifi 96:0d:cb:ff:f4:d0 -89  11      Y  US NONE
                        2WIRE341 00:22:a4:dd:8c:c9 -85  9       N  US WEP
                       HOME-F4D2 90:0d:cb:ff:f4:d0 -89  11      Y  US
WPA(PSK/TKIP,AES/TKIP) WPA2(PSK/TKIP,AES/TKIP)
                     xfinitywifi 74:85:2a:80:f5:e1 -91  157     Y  US NONE
                          HOME-5 74:85:2a:80:f5:e0 -91  157     Y  US
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                     BenjiNet_5G 2c:56:dc:85:3e:ec -57  157     Y  -- WPA2(PSK/AES/AES)
   DIRECT-F0-HP ENVY 7640 series a0:8c:fd:72:68:f1 -77  6       Y  -- WPA2(PSK/AES/AES)
                        linkysys 00:06:25:4b:21:b4 -46  5       N  -- WPA(PSK/AES/AES)
                        HOME-2.4 74:85:2a:80:f5:d8 -86  1       Y  US
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                          ATT288 3c:36:e4:22:95:80 -70  1       Y  --
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                    uLab-WiFiNet 4c:5e:0c:ca:25:c0 -37  1,+1    Y  -- WPA2(PSK/AES/AES)
      HP-Print-7B-Officejet 6600 6c:3b:e5:00:53:7b -87  9       N  -- WPA2(PSK/AES/AES)
                           Guest d8:50:e6:59:0b:fa -86  8       Y  -- WPA2(PSK/AES/AES)
                          Shauna d8:50:e6:59:0b:f9 -87  8       Y  -- WPA2(PSK/AES/AES)
                         MODWARE d8:50:e6:59:0b:f8 -86  8       Y  -- WPA2(PSK/AES/AES)
                        BenjiNet 2c:56:dc:85:3e:e8 -44  8       Y  -- WPA2(PSK/AES/AES)
Richards-MBP:~ rsimms$
```

On a Mac the built in airport command with an -s option will scan all available WiFi networks.

Activity

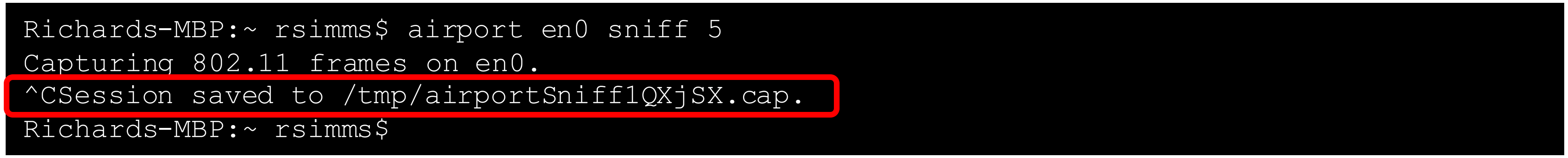
Look at the **airport -s** output on the previous slide

1) Is the Guest SSID network none, WEP, WPA or WPA2?

Write your answer in the chat window.

Sniffing using MacBook Pro

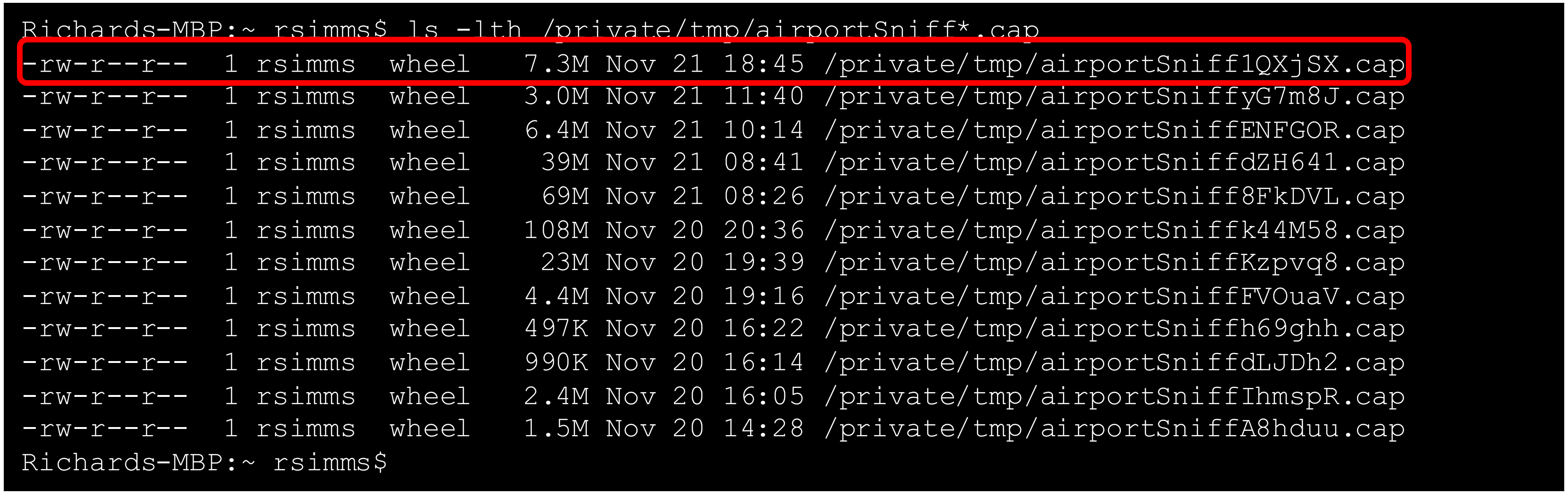
[on MacBook Pro] airport en0 sniff 5



```
Richards-MBP:~ rsimms$ airport en0 sniff 5
Capturing 802.11 frames on en0.
^CSession saved to /tmp/airportSniff1QXjSX.cap.
Richards-MBP:~ rsimms$
```

Let's start sniffing the channel used by the access point for the SSID linkysys. Use control-C to stop the capture.

[on MacBook Pro] ls -lth /private/tmp/airportSniff*.cap



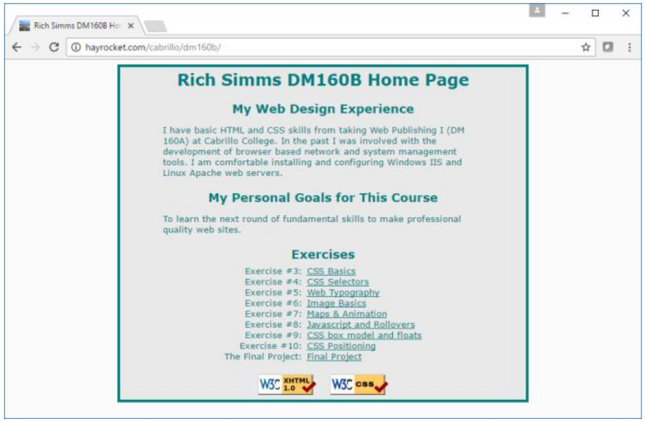
```
Richards-MBP:~ rsimms$ ls -lth /private/tmp/airportSniff*.cap
-rw-r--r--  1 rsimms  wheel   7.3M Nov 21 18:45 /private/tmp/airportSniff1QXjSX.cap
-rw-r--r--  1 rsimms  wheel   3.0M Nov 21 11:40 /private/tmp/airportSniffyG7m8J.cap
-rw-r--r--  1 rsimms  wheel   6.4M Nov 21 10:14 /private/tmp/airportSniffENFGOR.cap
-rw-r--r--  1 rsimms  wheel    39M Nov 21 08:41 /private/tmp/airportSniffdZH641.cap
-rw-r--r--  1 rsimms  wheel    69M Nov 21 08:26 /private/tmp/airportSniff8FkDVL.cap
-rw-r--r--  1 rsimms  wheel   108M Nov 20 20:36 /private/tmp/airportSniffk44M58.cap
-rw-r--r--  1 rsimms  wheel    23M Nov 20 19:39 /private/tmp/airportSniffKzpvq8.cap
-rw-r--r--  1 rsimms  wheel   4.4M Nov 20 19:16 /private/tmp/airportSniffFVOuaV.cap
-rw-r--r--  1 rsimms  wheel   497K Nov 20 16:22 /private/tmp/airportSniffh69ghh.cap
-rw-r--r--  1 rsimms  wheel   990K Nov 20 16:14 /private/tmp/airportSniffdLJDh2.cap
-rw-r--r--  1 rsimms  wheel   2.4M Nov 20 16:05 /private/tmp/airportSniffIhmspR.cap
-rw-r--r--  1 rsimms  wheel   1.5M Nov 20 14:28 /private/tmp/airportSniffA8hduu.cap
Richards-MBP:~ rsimms$
```

The packets are captured and dumped into a new file in the /private/tmp directory

Capture

1QXjSX

airportSniff1QXjSX.cap



Rich Simms DM160B Home Page

My Web Design Experience

I have basic HTML and CSS skills from taking Web Publishing I (DM 160A) at Cabrillo College. In the past I was involved with the development of browser based network and system management tools. I am comfortable installing and configuring Windows IIS and Linux Apache web servers.

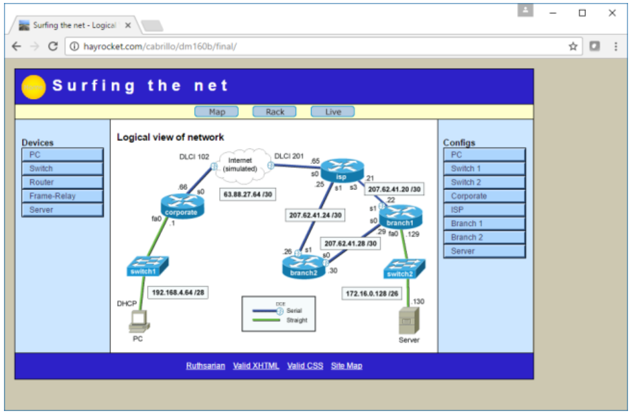
My Personal Goals for This Course

To learn the next round of fundamental skills to make professional quality web sites.

Exercises

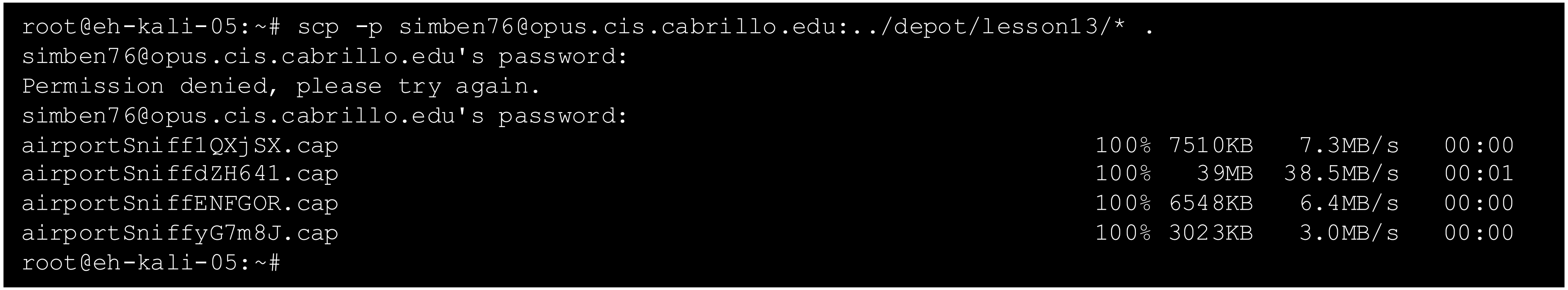
Exercise #3: CSS Basics
Exercise #4: CSS Selectors
Exercise #5: Web Typography
Exercise #6: Image Basics
Exercise #7: Maps & Animation
Exercise #8: Javascript and Rollovers
Exercise #9: CSS box model and floats
Exercise #10: CSS Positioning
The Final Project: Final Project

http://hayrocket.com/cabrillo/dm160b/



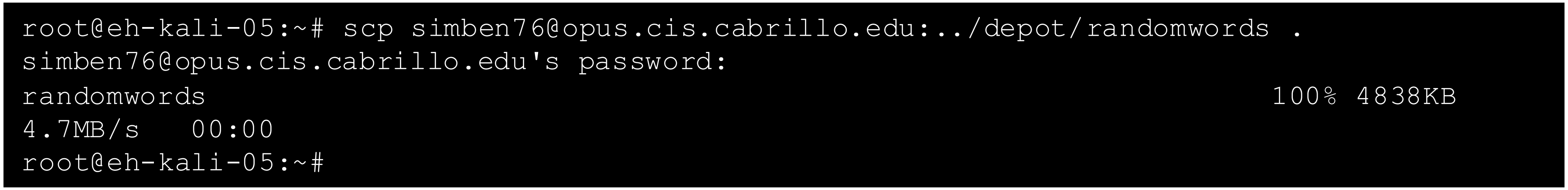
http://hayrocket.com/cabrillo/dm160b/final/

scp -p xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .



```
root@eh-kali-05:~# scp -p simben76@opus.cis.cabrillo.edu:../depot/lesson13/* .
simben76@opus.cis.cabrillo.edu's password:
Permission denied, please try again.
simben76@opus.cis.cabrillo.edu's password:
airportSniff1QXjSX.cap                                    100% 7510KB   7.3MB/s   00:00
airportSniffdZH641.cap                                    100%   39MB  38.5MB/s   00:01
airportSniffENFGOR.cap                                    100% 6548KB   6.4MB/s   00:00
airportSniffyG7m8J.cap                                    100% 3023KB   3.0MB/s   00:00
root@eh-kali-05:~#
```

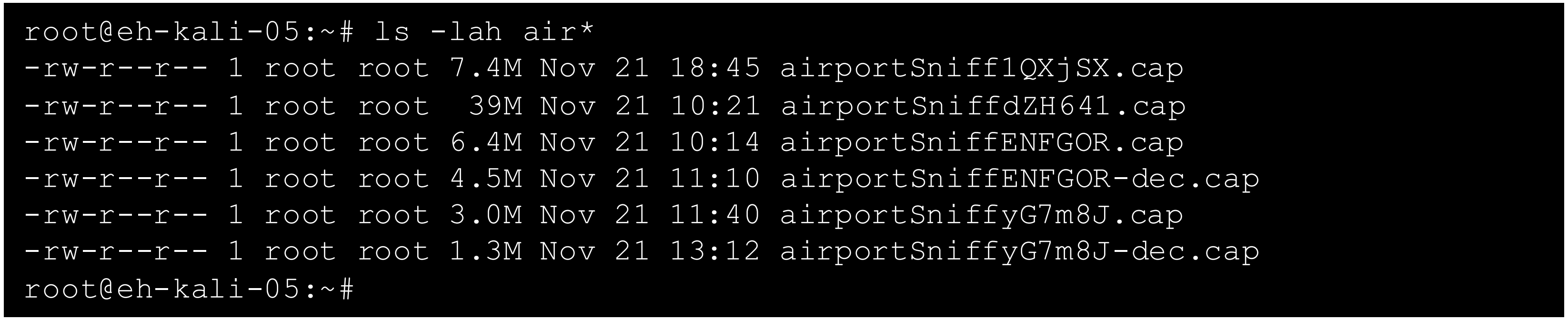
scp xxxxxx76@opus.cis.cabrillo.edu:../depot/randomwords .



```
root@eh-kali-05:~# scp simben76@opus.cis.cabrillo.edu:../depot/randomwords .
simben76@opus.cis.cabrillo.edu's password:
randomwords                                           100% 4838KB
4.7MB/s   00:00
root@eh-kali-05:~#
```

Obtain the packet captures files and word list

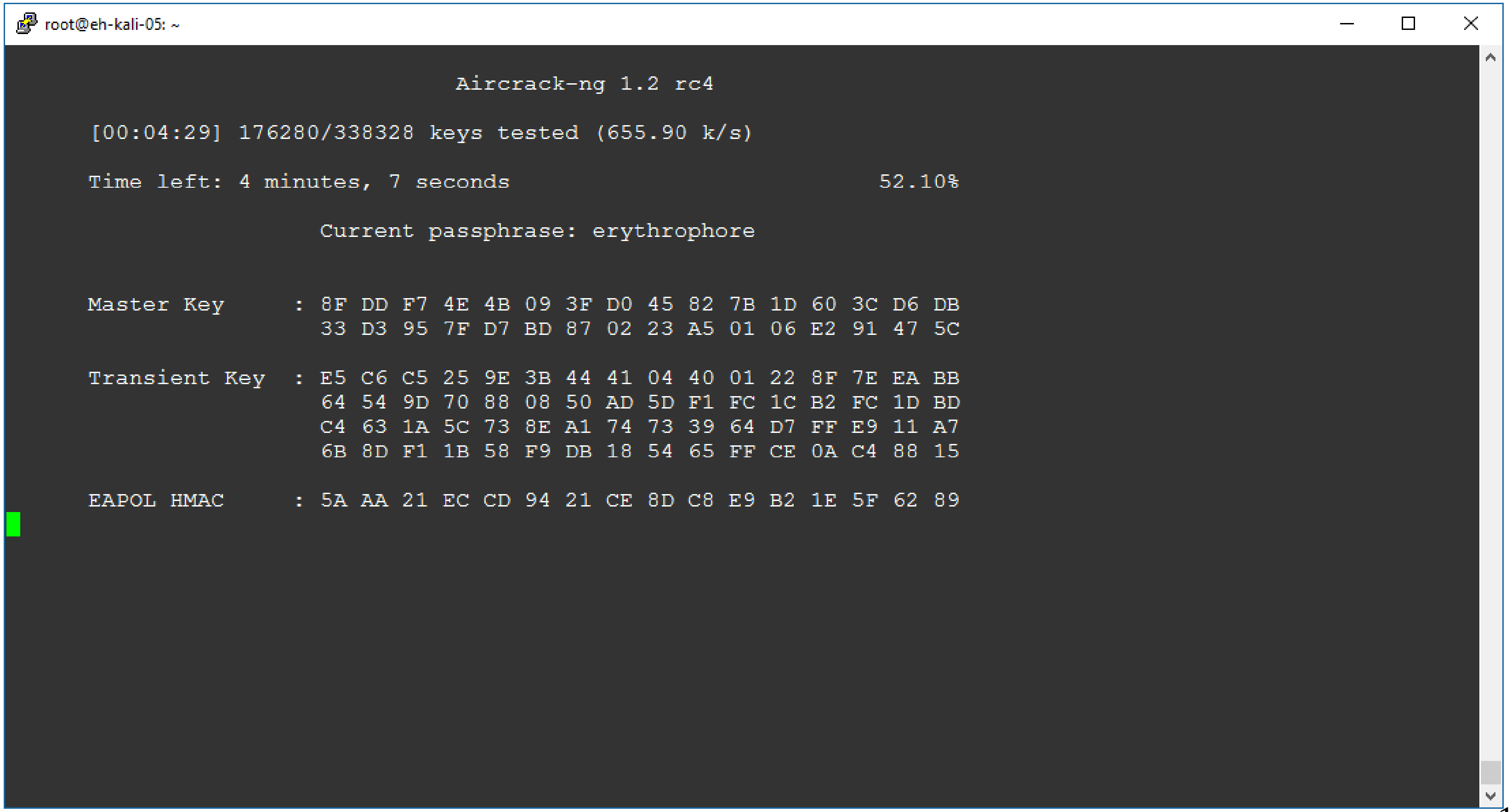
ls -lah air*



```
root@eh-kali-05:~# ls -lah air*
-rw-r--r-- 1 root root 7.4M Nov 21 18:45 airportSniff1QXjSX.cap
-rw-r--r-- 1 root root  39M Nov 21 10:21 airportSniffdZH641.cap
-rw-r--r-- 1 root root 6.4M Nov 21 10:14 airportSniffENFGOR.cap
-rw-r--r-- 1 root root 4.5M Nov 21 11:10 airportSniffENFGOR-dec.cap
-rw-r--r-- 1 root root 3.0M Nov 21 11:40 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 1.3M Nov 21 13:12 airportSniffyG7m8J-dec.cap
root@eh-kali-05:~#
```

Obtain the packet captures files and word list

```
aircrack-ng airportSniff1QXjSX.cap -w randomwords -b 00:06:25:4B:21:B4

Opening airportSniff1QXjSX.cap
Reading packets, please wait...
```



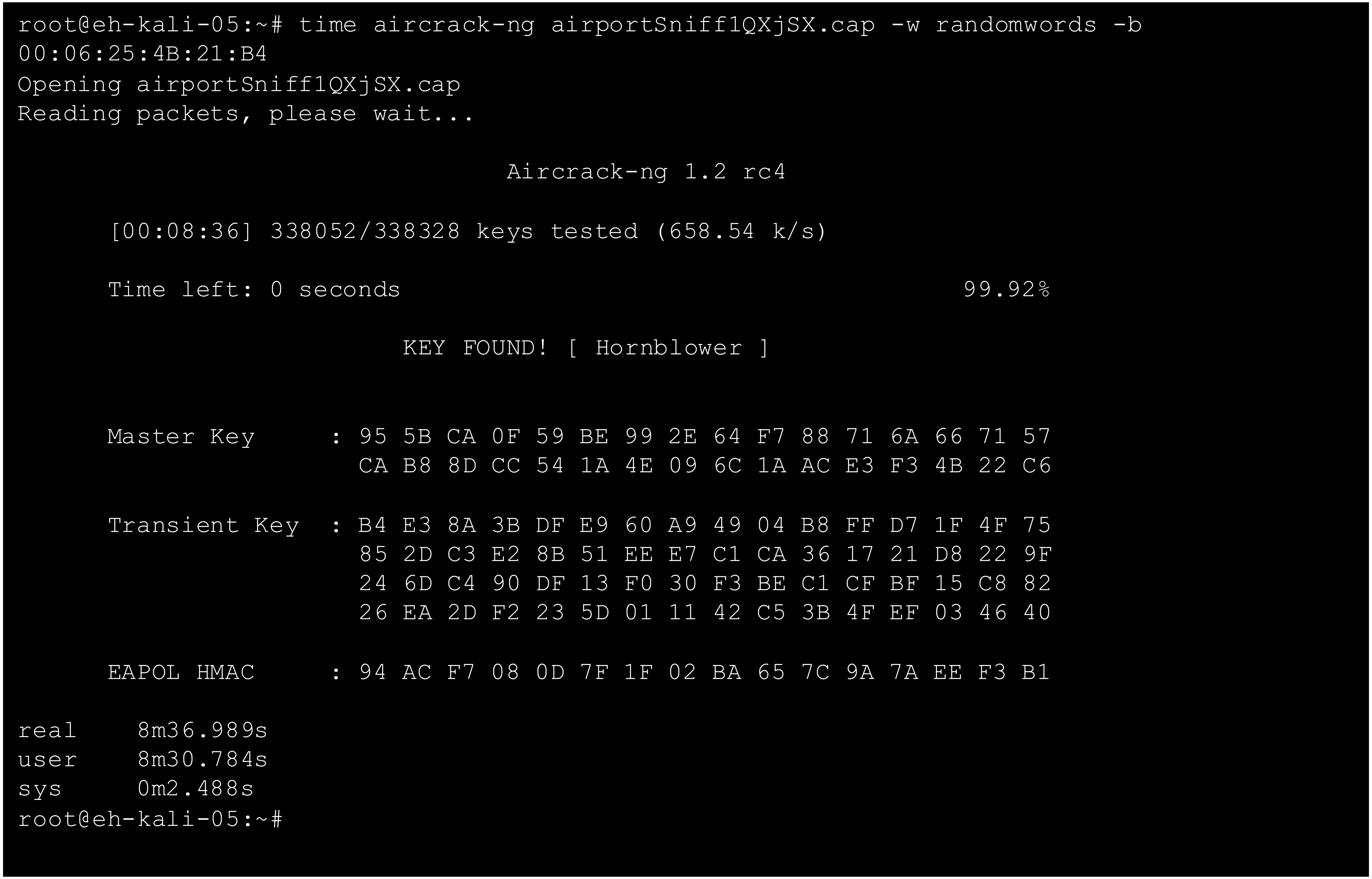
```
                              Aircrack-ng 1.2 rc4

      [00:04:29] 176280/338328 keys tested (655.90 k/s)

      Time left: 4 minutes, 7 seconds                           52.10%

                       Current passphrase: erythrophore


      Master Key     : 8F DD F7 4E 4B 09 3F D0 45 82 7B 1D 60 3C D6 DB
                       33 D3 95 7F D7 BD 87 02 23 A5 01 06 E2 91 47 5C

      Transient Key  : E5 C6 C5 25 9E 3B 44 41 04 40 01 22 8F 7E EA BB
                       64 54 9D 70 88 08 50 AD 5D F1 FC 1C B2 FC 1D BD
                       C4 63 1A 5C 73 8E A1 74 73 39 64 D7 FF E9 11 A7
                       6B 8D F1 1B 58 F9 DB 18 54 65 FF CE 0A C4 88 15

      EAPOL HMAC     : 5A AA 21 EC CD 94 21 CE 8D C8 E9 B2 1E 5F 62 89
```

Activity

As root, on your EH-Kali-XX VM:

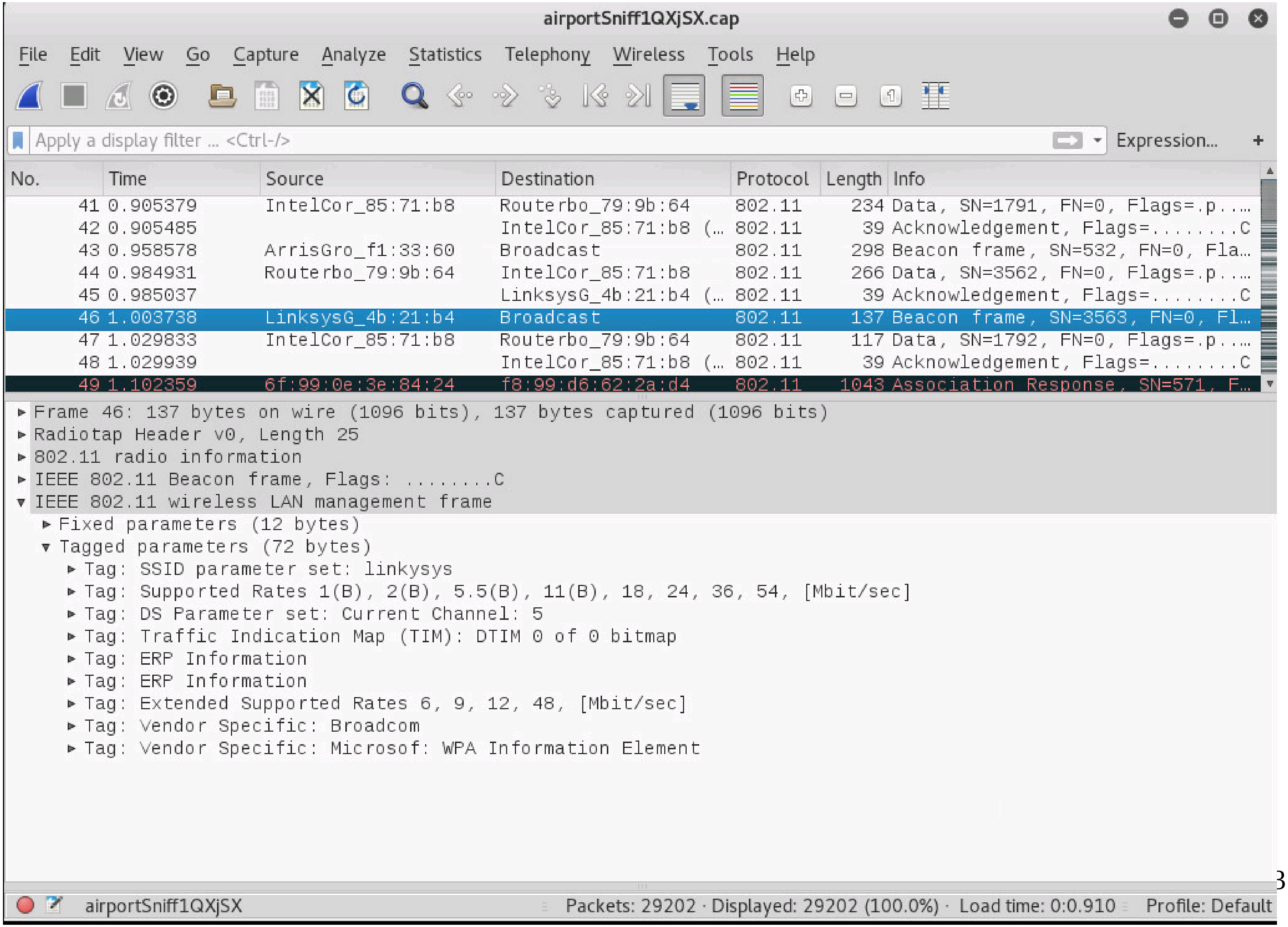
```
scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .
scp xxxxxx76@opus.cis.cabrillo.edu:../depot/randomwords .

aircrack-ng airportSniff1QXjSX.cap -w randomwords -b 00:06:25:4B:21:B4
```

What is the WPA shared key? Write your answer in the chat window



```
root@eh-kali-05:~# time aircrack-ng airportSniff1QXjSX.cap -w randomwords -b
00:06:25:4B:21:B4
Opening airportSniff1QXjSX.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc4

      [00:08:36] 338052/338328 keys tested (658.54 k/s)

      Time left: 0 seconds                                      99.92%

                          KEY FOUND! [ Hornblower ]


      Master Key     : 95 5B CA 0F 59 BE 99 2E 64 F7 88 71 6A 66 71 57
                       CA B8 8D CC 54 1A 4E 09 6C 1A AC E3 F3 4B 22 C6

      Transient Key  : B4 E3 8A 3B DF E9 60 A9 49 04 B8 FF D7 1F 4F 75
                       85 2D C3 E2 8B 51 EE E7 C1 CA 36 17 21 D8 22 9F
                       24 6D C4 90 DF 13 F0 30 F3 BE C1 CF BF 15 C8 82
                       26 EA 2D F2 23 5D 01 11 42 C5 3B 4F EF 03 46 40

      EAPOL HMAC     : 94 AC F7 08 0D 7F 1F 02 BA 65 7C 9A 7A EE F3 B1

real    8m36.989s
user    8m30.784s
sys     0m2.488s
root@eh-kali-05:~#
```

Using time to see how long it takes

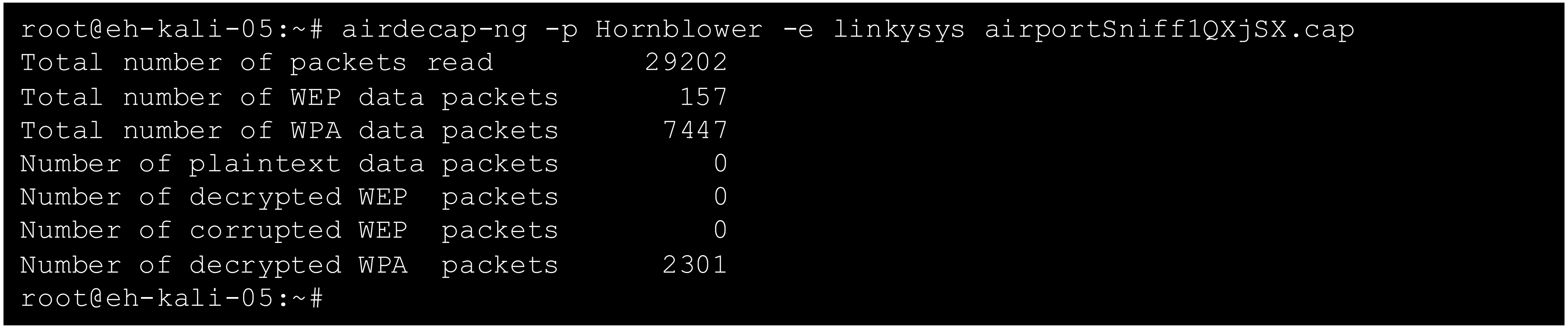


```
No.   Time        Source              Destination            Protocol  Length Info
   41 0.905379    IntelCor_85:71:b8   Routerbo_79:9b:64      802.11     234 Data, SN=1791, FN=0, Flags=.p.…
   42 0.905485                        IntelCor_85:71:b8 (…  802.11      39 Acknowledgement, Flags=........C
   43 0.958578    ArrisGro_f1:33:60   Broadcast              802.11     298 Beacon frame, SN=532, FN=0, Fla…
   44 0.984931    Routerbo_79:9b:64   IntelCor_85:71:b8      802.11     266 Data, SN=3562, FN=0, Flags=.p.…
   45 0.985037                        LinksysG_4b:21:b4 (…  802.11      39 Acknowledgement, Flags=........C
   46 1.003738    LinksysG_4b:21:b4   Broadcast              802.11     137 Beacon frame, SN=3563, FN=0, Fl…
   47 1.029833    IntelCor_85:71:b8   Routerbo_79:9b:64      802.11     117 Data, SN=1792, FN=0, Flags=.p.…
   48 1.029939                        IntelCor_85:71:b8 (…  802.11      39 Acknowledgement, Flags=........C
   49 1.102359    6f:99:0e:3e:84:24   f8:99:d6:62:2a:d4      802.11    1043 Association Response, SN=571, F…
```

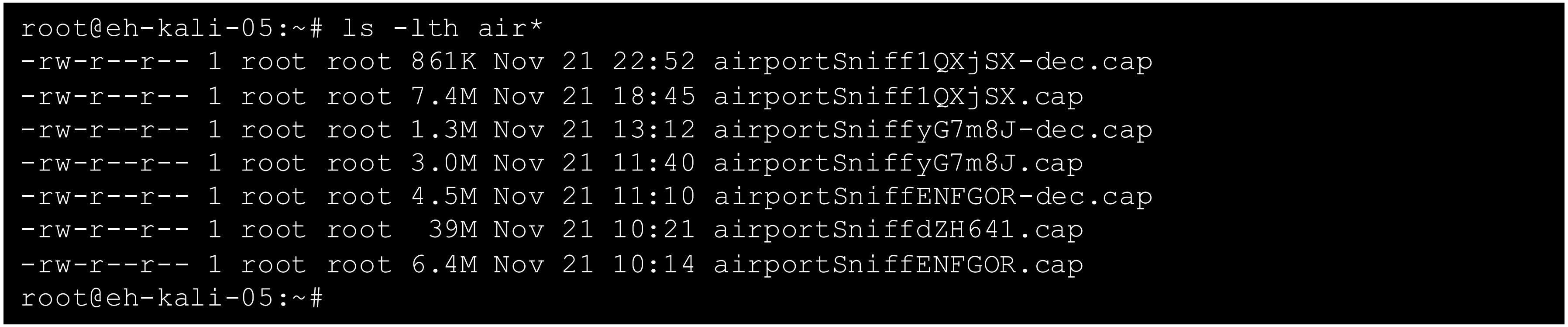
```
▶ Frame 46: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: ........C
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (72 bytes)
    ▶ Tag: SSID parameter set: linkysys
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 5
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
    ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▶ Tag: Vendor Specific: Broadcom
    ▶ Tag: Vendor Specific: Microsof: WPA Information Element
```

airportSniff1QXjSX Packets: 29202 · Displayed: 29202 (100.0%) · Load time: 0:0.910 Profile: Default

airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap



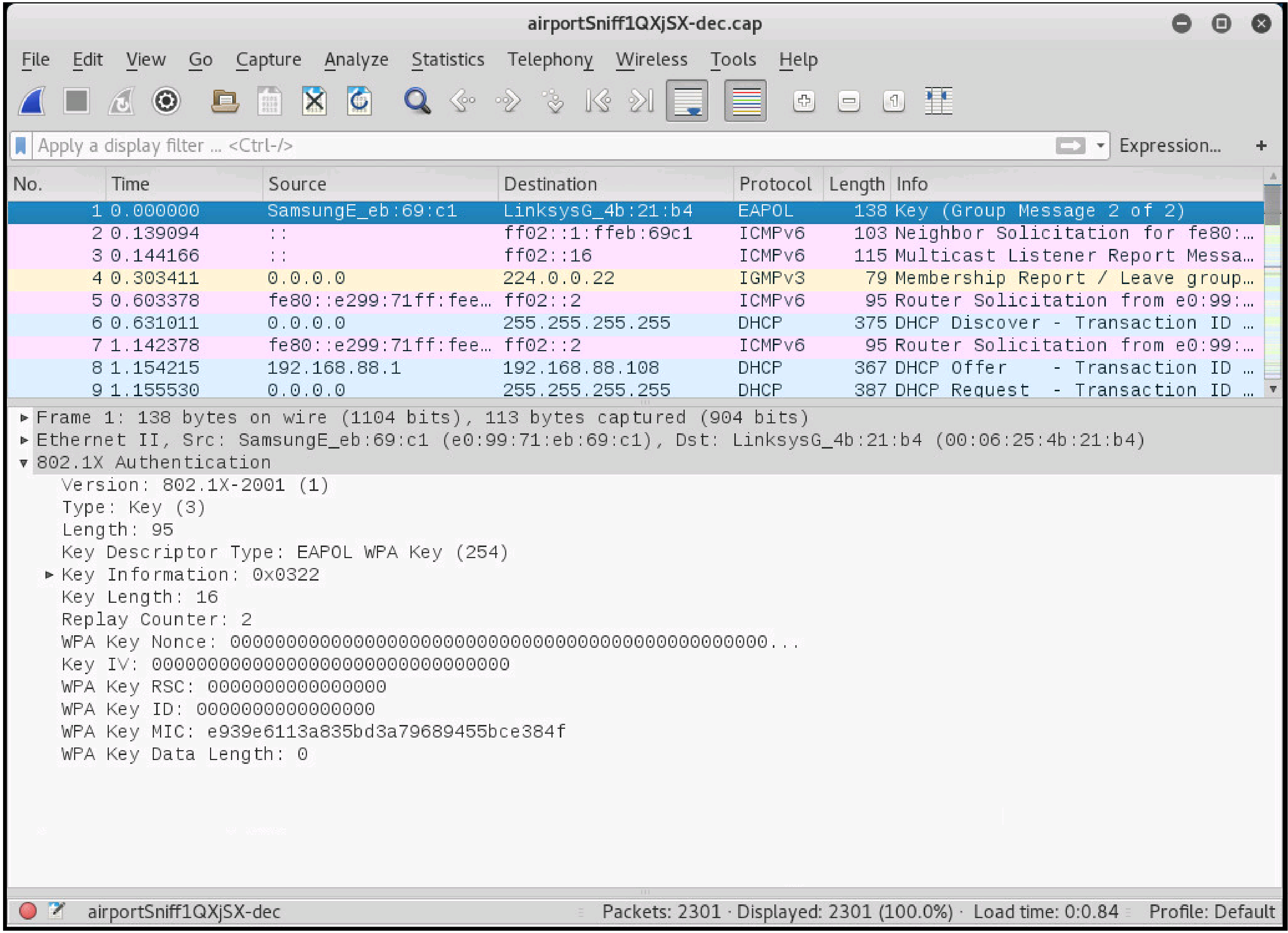
```
root@eh-kali-05:~# airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap
Total number of packets read         29202
Total number of WEP data packets       157
Total number of WPA data packets      7447
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      2301
root@eh-kali-05:~#
```



```
root@eh-kali-05:~# ls -lth air*
-rw-r--r-- 1 root root 861K Nov 21 22:52 airportSniff1QXjSX-dec.cap
-rw-r--r-- 1 root root 7.4M Nov 21 18:45 airportSniff1QXjSX.cap
-rw-r--r-- 1 root root 1.3M Nov 21 13:12 airportSniffyG7m8J-dec.cap
-rw-r--r-- 1 root root 3.0M Nov 21 11:40 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 4.5M Nov 21 11:10 airportSniffENFGOR-dec.cap
-rw-r--r-- 1 root root  39M Nov 21 10:21 airportSniffdZH641.cap
-rw-r--r-- 1 root root 6.4M Nov 21 10:14 airportSniffENFGOR.cap
root@eh-kali-05:~#
```

Decrypt the packet capture file

CIS 76 - Lesson 13

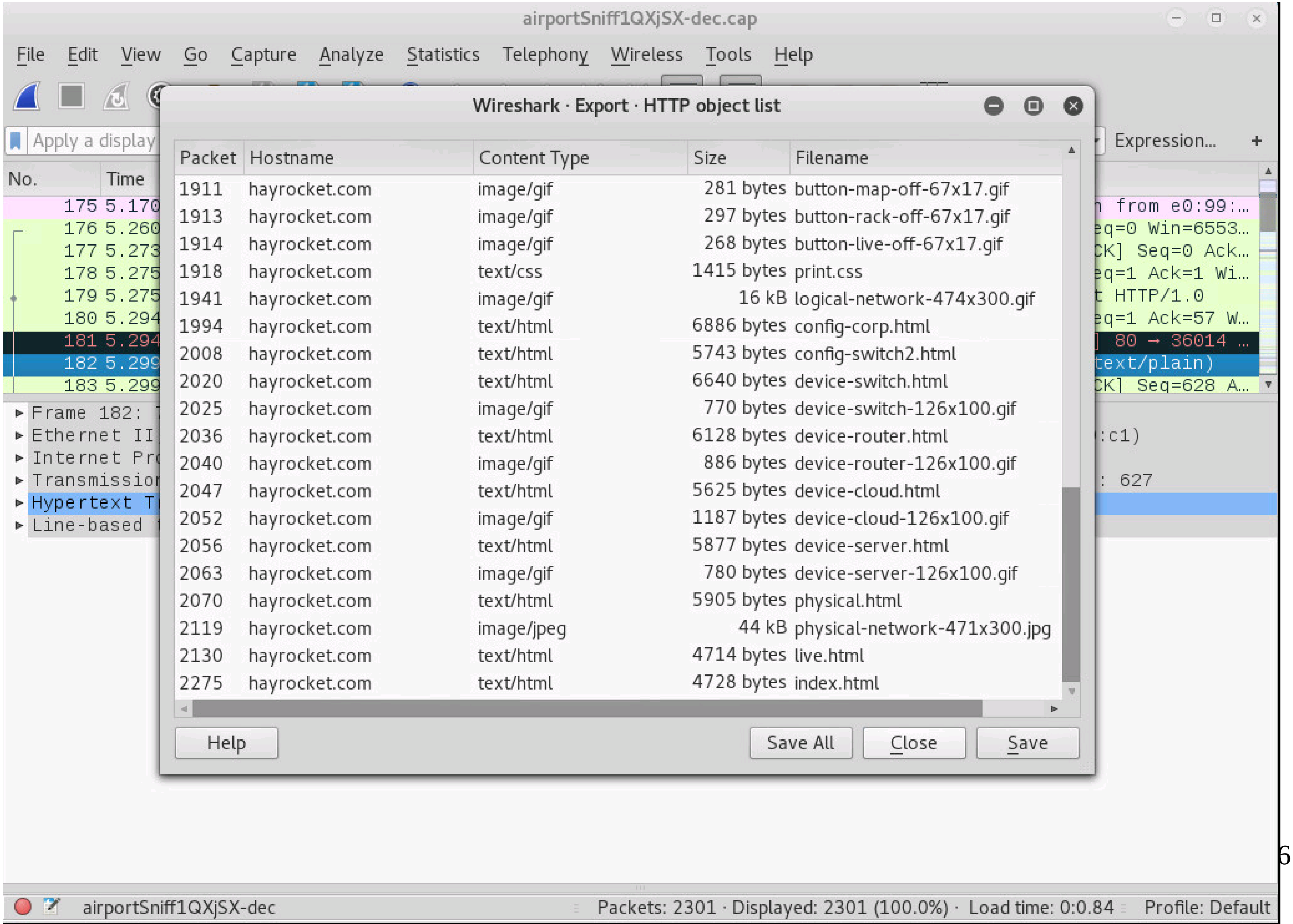


airportSniff1QXjSX-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source                    Destination          Protocol Length Info
   1 0.000000  SamsungE_eb:69:c1         LinksysG_4b:21:b4    EAPOL       138 Key (Group Message 2 of 2)
   2 0.139094  ::                        ff02::1:ffeb:69c1    ICMPv6      103 Neighbor Solicitation for fe80:…
   3 0.144166  ::                        ff02::16             ICMPv6      115 Multicast Listener Report Messa…
   4 0.303411  0.0.0.0                   224.0.0.22           IGMPv3       79 Membership Report / Leave group…
   5 0.603378  fe80::e299:71ff:fee…      ff02::2              ICMPv6       95 Router Solicitation from e0:99:…
   6 0.631011  0.0.0.0                   255.255.255.255      DHCP        375 DHCP Discover - Transaction ID …
   7 1.142378  fe80::e299:71ff:fee…      ff02::2              ICMPv6       95 Router Solicitation from e0:99:…
   8 1.154215  192.168.88.1              192.168.88.108       DHCP        367 DHCP Offer    - Transaction ID …
   9 1.155530  0.0.0.0                   255.255.255.255      DHCP        387 DHCP Request  - Transaction ID …
```

```
▸ Frame 1: 138 bytes on wire (1104 bits), 113 bytes captured (904 bits)
▸ Ethernet II, Src: SamsungE_eb:69:c1 (e0:99:71:eb:69:c1), Dst: LinksysG_4b:21:b4 (00:06:25:4b:21:b4)
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▸ Key Information: 0x0322
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 000000000000000000000000000000000000000000000000...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: e939e6113a835bd3a79689455bce384f
    WPA Key Data Length: 0
```

airportSniff1QXjSX-dec   Packets: 2301 · Displayed: 2301 (100.0%) · Load time: 0:0.84   Profile: Default



airportSniff1QXjSX-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display
Expression...
No. Time
Wireshark · Export · HTTP object list
Help
Save All
Close
Save

Packet	Hostname	Content Type	Size	Filename
1911	hayrocket.com	image/gif	281 bytes	button-map-off-67x17.gif
1913	hayrocket.com	image/gif	297 bytes	button-rack-off-67x17.gif
1914	hayrocket.com	image/gif	268 bytes	button-live-off-67x17.gif
1918	hayrocket.com	text/css	1415 bytes	print.css
1941	hayrocket.com	image/gif	16 kB	logical-network-474x300.gif
1994	hayrocket.com	text/html	6886 bytes	config-corp.html
2008	hayrocket.com	text/html	5743 bytes	config-switch2.html
2020	hayrocket.com	text/html	6640 bytes	device-switch.html
2025	hayrocket.com	image/gif	770 bytes	device-switch-126x100.gif
2036	hayrocket.com	text/html	6128 bytes	device-router.html
2040	hayrocket.com	image/gif	886 bytes	device-router-126x100.gif
2047	hayrocket.com	text/html	5625 bytes	device-cloud.html
2052	hayrocket.com	image/gif	1187 bytes	device-cloud-126x100.gif
2056	hayrocket.com	text/html	5877 bytes	device-server.html
2063	hayrocket.com	image/gif	780 bytes	device-server-126x100.gif
2070	hayrocket.com	text/html	5905 bytes	physical.html
2119	hayrocket.com	image/jpeg	44 kB	physical-network-471x300.jpg
2130	hayrocket.com	text/html	4714 bytes	live.html
2275	hayrocket.com	text/html	4728 bytes	index.html

airportSniff1QXjSX-dec Packets: 2301 · Displayed: 2301 (100.0%) · Load time: 0:0.84 Profile: Default

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap**

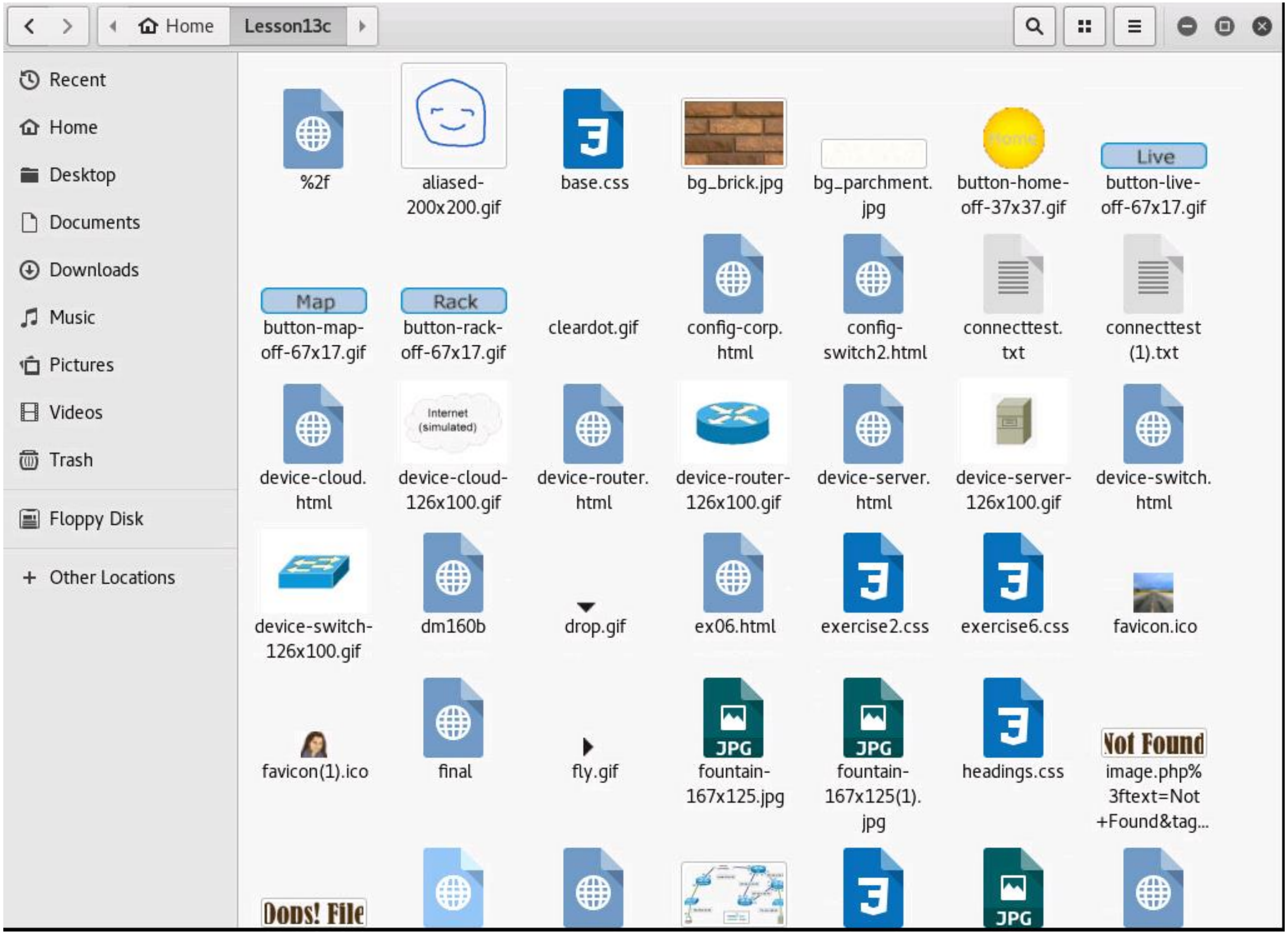
3) Run Wireshark on the decrypted airportSniff1QXjSX-dec.cap file.

4) File > Export Objects > HTTP

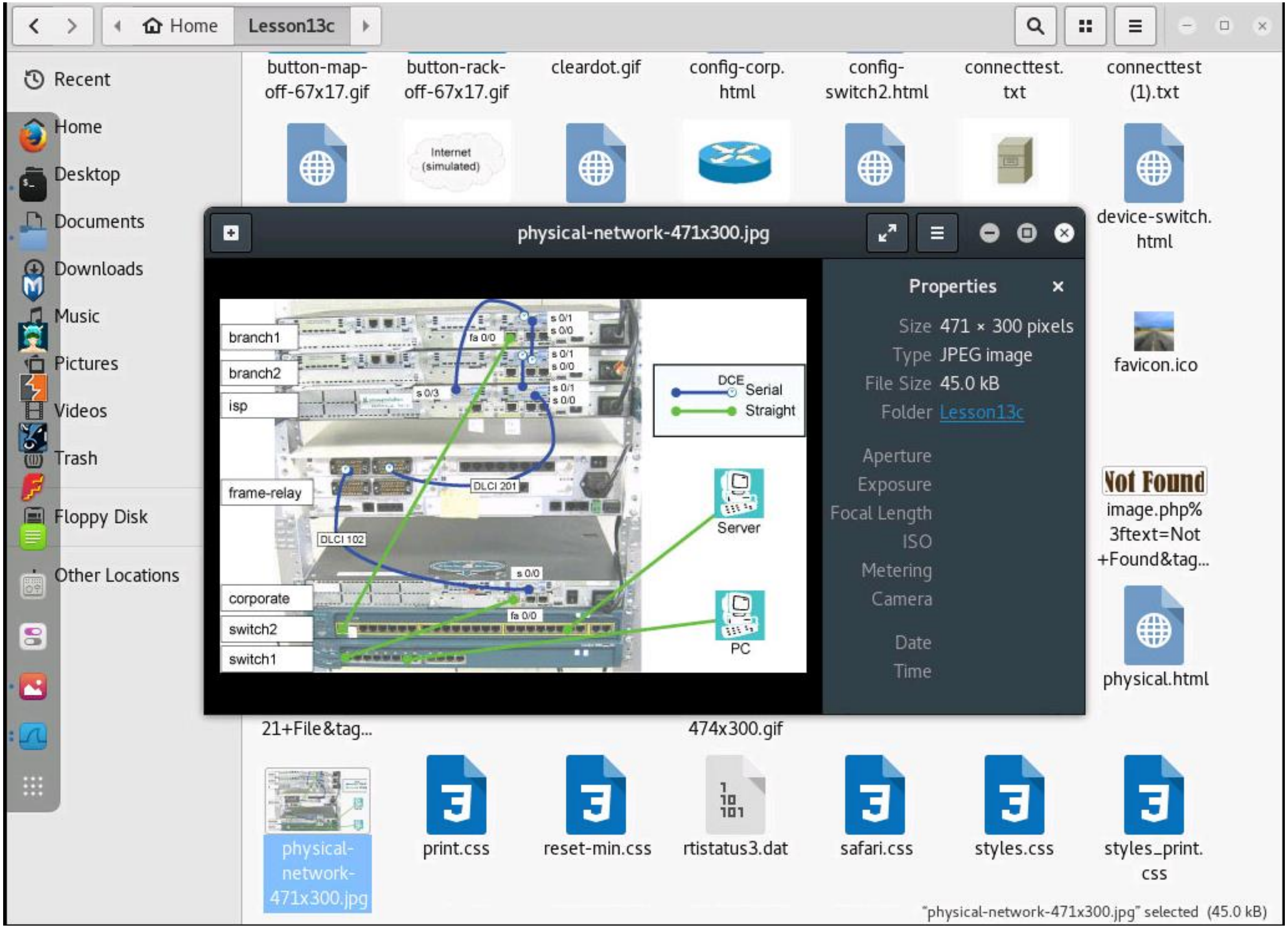
5) Create a new lesson13c directory.

6) Save all the objects in the new directory.

When finished note it in the chat window.



%2f
aliased-200x200.gif
base.css
bg_brick.jpg
bg_parchment.jpg
button-home-off-37x37.gif
button-live-off-67x17.gif
button-map-off-67x17.gif
button-rack-off-67x17.gif
cleardot.gif
config-corp.html
config-switch2.html
connecttest.txt
connecttest (1).txt
device-cloud.html
device-cloud-126x100.gif
device-router.html
device-router-126x100.gif
device-server.html
device-server-126x100.gif
device-switch.html
device-switch-126x100.gif
dm160b
drop.gif
ex06.html
exercise2.css
exercise6.css
favicon.ico
favicon(1).ico
final
fly.gif
fountain-167x125.jpg
fountain-167x125(1).jpg
headings.css
image.php%3ftext=Not+Found&tag...



button-map-off-67x17.gif

button-rack-off-67x17.gif

cleardot.gif

config-corp.html

config-switch2.html

connecttest.txt

connecttest (1).txt

device-switch.html

favicon.ico

image.php%3ftext=Not+Found&tag...

physical.html

21+File&tag...

474x300.gif

physical-network-471x300.jpg

print.css

reset-min.css

rtistatus3.dat

safari.css

styles.css

styles_print.css

physical-network-471x300.jpg

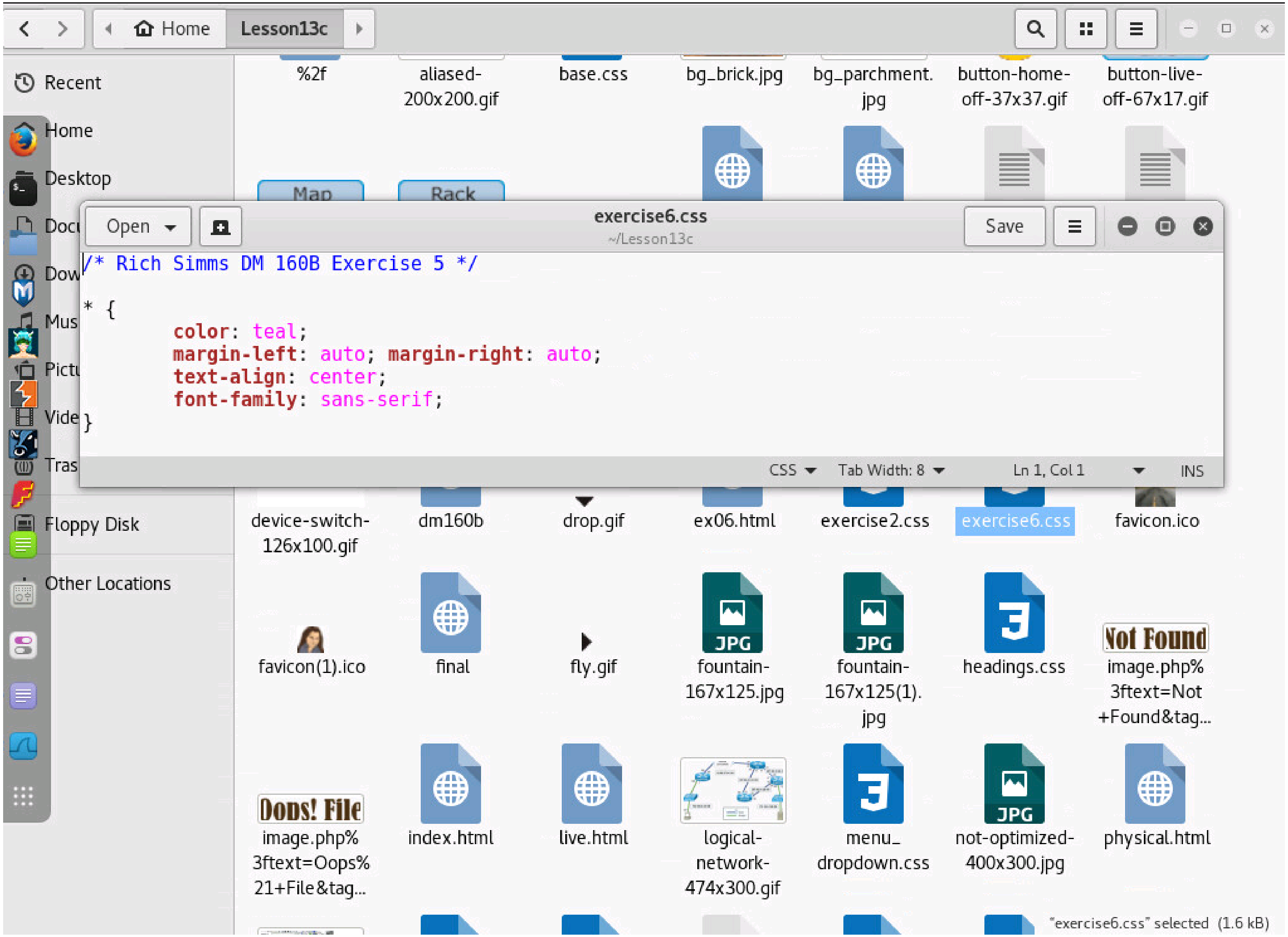
Properties

Size 471 × 300 pixels
Type JPEG image
File Size 45.0 kB
Folder Lesson13c

Aperture
Exposure
Focal Length
ISO
Metering
Camera

Date
Time

"physical-network-471x300.jpg" selected (45.0 kB)

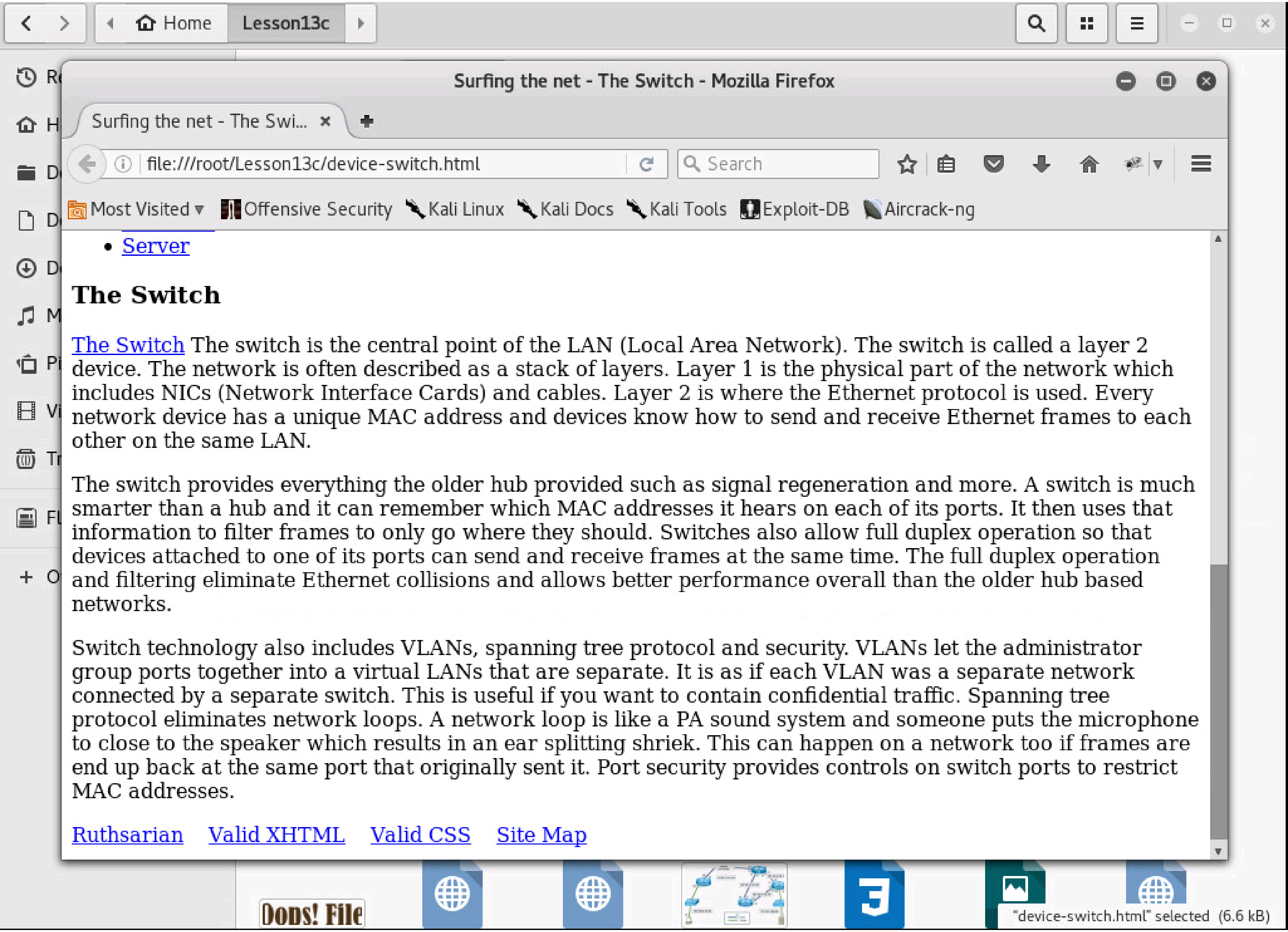


exercise6.css
~/Lesson13c

```
/* Rich Simms DM 160B Exercise 5 */

* {
	color: teal;
	margin-left: auto; margin-right: auto;
	text-align: center;
	font-family: sans-serif;
}
```

CSS Tab Width: 8 Ln 1, Col 1 INS

"exercise6.css" selected (1.6 kB)


Home
Lesson13c
Surfing the net - The Switch - Mozilla Firefox
Surfing the net - The Swi...
file:///root/Lesson13c/device-switch.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Oops! File
"device-switch.html" selected (6.6 kB)

- Server

The Switch

The Switch The switch is the central point of the LAN (Local Area Network). The switch is called a layer 2 device. The network is often described as a stack of layers. Layer 1 is the physical part of the network which includes NICs (Network Interface Cards) and cables. Layer 2 is where the Ethernet protocol is used. Every network device has a unique MAC address and devices know how to send and receive Ethernet frames to each other on the same LAN.

The switch provides everything the older hub provided such as signal regeneration and more. A switch is much smarter than a hub and it can remember which MAC addresses it hears on each of its ports. It then uses that information to filter frames to only go where they should. Switches also allow full duplex operation so that devices attached to one of its ports can send and receive frames at the same time. The full duplex operation and filtering eliminate Ethernet collisions and allows better performance overall than the older hub based networks.

Switch technology also includes VLANs, spanning tree protocol and security. VLANs let the administrator group ports together into a virtual LANs that are separate. It is as if each VLAN was a separate network connected by a separate switch. This is useful if you want to contain confidential traffic. Spanning tree protocol eliminates network loops. A network loop is like a PA sound system and someone puts the microphone to close to the speaker which results in an ear splitting shriek. This can happen on a network too if frames are end up back at the same port that originally sent it. Port security provides controls on switch ports to restrict MAC addresses.

Ruthsarian Valid XHTML Valid CSS Site Map

Activity

As root, on your EH-Kali-XX VM:

1) Find the extracted config-switch2.html file.

2) What is the password used on this switch?

Write your answer in the chat window.

Assignment

Final Project

Cabrillo College

CIS 76 Linux Lab Exercise

Final Project
Fall 2016

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

Due in two weeks

Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Final project due in two weeks

Quiz questions for next class:

- No more quizzes!

Backup